UNIVERSITÀ DEGLI STUDI DI TRENTO

Facoltà di Giurisprudenza

Corso di Laurea Magistrale in Giurisprudenza

LA FRODE INFORMATICA NEL QUADRO DELLA DISCIPLINA NAZIONALE E COMPARATA. PROSPETTIVE DE IURE CONDENDO

Relatore:

Prof. Alessandro Melchionda

Laureanda:

Erica Vicentini

Anno Accademico: 2014-2015

Parole chiave: diritto penale dell’informatica, frode informatica, identità digitale, patrimonializzazione dei dati, “phishing”.

INDICE

Introduzione

La diffusione delle tecnologie informatiche ha raggiunto negli ultimi anni livelli globali ed ha obbligato i legislatori e gli operatori del diritto a fare i conti con essa. Il fondamento di tale vertiginoso sviluppo risiede non solo nel progresso della ricerca scientifica ma anche e soprattutto nella straordinaria capacità dell'"*Information Communication Technology*" (I.C.T.) di soddisfare le esigenze organizzative e gestionali sia di soggetti privati sia di soggetti pubblici.
È possibile individuare in primis una dimensione "fisiologica" dello sviluppo tecnologico-digitale. Le pubbliche amministrazioni e le imprese private hanno elaborato modelli di gestione nuovi, altamente efficienti e dai costi umani spesso molto contenuti, i quali hanno come *leit motiv* proprio la loro "virtualità". L'informatizzazione dei processi produttivi e delle relazioni sociali e la conseguente dematerializzazione dei beni percepiti come meritevoli di tutela ha investito pressoché tutti i settori della società contemporanea: dal settore privato al sistema sanitario, i trasporti pubblici di terra, i trasporti aerei, i sistemi bancari e di telecomunicazioni.
L'economia globale ha subito notevoli cambiamenti con la digitalizzazione dei processi produttivi e del marketing pubblicitario: le nuove tecnologie hanno permesso anche alle piccole e medie imprese di espandere la propria rete commerciale oltre i confini nazionali, riducendo drasticamente le barriere spaziali e temporali. Hanno generato inoltre figure professionali nuove, specializzate in nuove categorie di servizi, accelerando a volte la scomparsa di altre figure professionali più tradizionali.
Anche sui consumatori sono ricaduti grandi benefici dall'apertura del mercato attraverso la rete: oggi il commercio elettronico è una realtà in continua evoluzione che consente una scelta quasi infinita di beni da ogni parte del mondo a costi a volte più convenienti di quelli degli esercizi commerciali in loco.
A livello sociale, le nuove tecnologie hanno aperto nuovi spazi per le attività ludiche e hanno eliminato quasi del tutto gli ostacoli nelle comunicazioni a distanza: la "società connessa" è realtà, oggi è possibile comunicare dati ed

informazioni in tempo reale in pressoché tutto il mondo a costi largamente sostenibili.

Parallelamente allo sviluppo fisiologico dell'I.C.T., si è avuto anche uno sviluppo "patologico": a partire dagli anni '70 hanno iniziato a diffondersi i c.d. *Computer crimes*, forme deliquenziali che si concretizzano in una lesione a beni giuridici personali e patrimoniali legati alla sicurezza nei sistemi informatici e dei dati in essi contenuti. Le prime condotte abusive a danno di un elaboratore elettronico furono i casi di c.d. *phone phreaking*, condotte di abuso delle nuove tecnologie per effettuare telefonate gratuite o a costi minori di quelli regolari.

Negli anni '80, con lo sviluppo e la diffusione di massa dei computer[1], furono sviluppate anche potenti forme di disturbo dell'utilizzo dei PC: nel 1988 Robert Morris creò un "*worm*"[2], un programma informatico in grado di autoreplicarsi e che in quell'occasione ha mandato in *loop* più di 6000 computer connessi (un decimo dei computer connessi ad internet in quel tempo).

Dalla metà degli anni '90, quando Internet si apre concretamente al pubblico diventando un fenomeno globale[3], il *Computer Crime* si evolve in *Cyber Crime*, lesione al bene giuridico informatico collocata nella rete globale, il c.d. *Cyber space*. Il rapporto non è più fra un soggetto e un oggetto fisico - PC: l'individuo

[1] IBM introdusse in quegli anni gli "IBM PC", i progenitori dei computer oggi comunemente usati, basati sui processori Intel 8088, affidabili e realizzati con prodotti normalmente reperibili sul mercato; erano però ancora costosi. Ciò portò in un brevissimo periodo alla realizzazione da parte di molte altre imprese di PC IBM-compatibili o similari, a prezzo ridotto con caratteristiche diverse e sempre più tecnologicamente sofisticate.

[2] Un *worm* è un particolare tipo di malicious software che non necessita di legarsi ad altri programmi eseguibili per diffondersi. Tenta di auto replicarsi sfruttando Internet in diversi modi (quello più comune è la posta elettronica): una volta introdottosi in un sistema operativo, lo infetta in modo tale da essere eseguito ogni volta che l'elaboratore viene avviato. Rimane attivo finché non viene spento il PC o arrestato il processo corrispondente.

[3] Comunemente si individua come data di nascita di Internet il 1 Gennaio 1983, quando la rete ARPANET, prima rete di connessione fra elaboratori informatici creata dal Dipartimento della Difesa USA - Agenzia ARPA (*Advanced Research Projects Agency*) per ampliare e sviluppare la ricerca con la collaborazione poi delle Università della California e dello Utah, cambiò il suo "*host protocol*" con "*Trasmission Control Protocol and Internet Protocol*": Internet permise di avere PC con una propria interfaccia utente che rimanesse comunque sempre connessa con il resto della rete. Nel 1993, dopo i primi due anni in cui fu utilizzato solo in ambito scientifico-accademico, fu messo a disposizione del pubblico il World Wide Web ("www"): si trattava di un software per la condivisione di documentazione scientifica indipendentemente dalla piattaforma, sviluppato da Tim Berners-Lee presso il CERN (Centro Europeo per la ricerca nucleare) di Ginevra. Ne era nata una rete di siti scritti in un linguaggio informatico più semplice dei precedenti noto come Hypertext Transfer Protocol ("http"). In pochissimi anni il WWW divenne la modalità più diffusa al mondo per inviare e ricevere dati su Internet: 150 siti Web apparvero già nel 1993, 3.000 nel 1994; 25.000 nel 1995; 25.0000 nel 1996 e nel giugno del 2000 erano 10 milioni

è in rapporto con una vera e propria dimensione (sociale, economica) in cui comportamenti anche singolarmente innocui possono diventare dannosi. Oggi la rete ha assunto una dimensione a pieno titolo globale e rappresenta talora un mondo virtuale parallelo, nel quale si infrangono le regole spazio-temporali tradizionali ed i limiti all'azione umana come fino ad oggi conosciuti.

L'intervento penale è richiesto in primis dagli ingenti danni economici causati da tali fenomeni. I virus informatici che hanno causato milioni (o addirittura bilioni) di dollari di danni sono stati molti negli anni: fra questi è sufficiente ricordare nel 1999 il virus "Melissa" e nel 2000 il virus-email "Love-Bug"[4]; o ancora, un "*denial-of-service attack*"[5] creato da un teen-ager canadese che fu in grado di inabilitare websites quali *Amazon* e *Yahoo!*. L'ultimo caso che è stato definito la più grande frode nella storia della finanza internazionale colpì la *Société Générale* (la seconda banca francese) nel gennaio 2008[6].

Secondariamente, anche l'anonimato di cui possono godere gli *hacker* informatici (è molto complesso infatti associare univocamente ad un computer un'identità personale e fisica), la diffusa tolleranza di tali comportamenti (che non sono percepiti come illeciti e dannosi dall'opinione pubblica non direttamente colpita), le difficoltà di investigazione (spesso si tratta di illeciti transfrontalieri che determinano la necessità di collaborazioni intergovernative) la sicurezza e la diffusa reperibilità di strumenti tecnologici come la crittografia (possono proteggere tutti quei documenti e comunicazioni che si desidera "nascondere"), infine la facilità ed economicità di utilizzo delle nuove tecnologie

[4] Il "virus" è un insieme di comandi in grado, una volta in esecuzione, di infettare i processi e i files all'interno di un elaboratore elettronico e di riprodursi, creando copie di sé stesso. Lo spostamento in altre macchine avviene attraverso il trasferimento di files infetti. Generalmente, quando l'utente lancia il programma infettato, viene prima eseguito il virus senza che l'utente se ne accorga, e poi il programma stesso. Il virus rimane in esecuzione nella memoria del PC e compie le varie operazioni contenute nel suo codice (possono essere le più disparate: copiare dati, bloccare il funzionamento di programmi o dell'intero elaboratore, far compiere operazioni alla macchina senza il previo comando da parte dell'utente, formattare l'hard-disk, far apparire messaggi, modificare l'interfaccia-utente); inoltre esegue copie di sé stesso al fine di "spargere l'epidemia".

[5] Nel *DDos attack*, vi è un soggetto attivo che usa un sistema informatico già compromesso per inviare enormi quantità di messaggi inabilitanti al computer-obiettivo.

[6] La Banca francese denunciò in tale occasione una perdita di 4,9 miliardi di euro. Il responsabile era un trader di 31 anni dipendente dell'istituto di credito che, sfruttando le proprie conoscenze informatiche, aveva avviato operazioni finanziarie ad alto rischio per tutto il 2007, causando così un buco nei conti del colosso bancario

sono caratteristiche che rendono gli illeciti informatici molto “appetibili” e quindi diffusi. Non a caso esperti criminologi quali Don Parker insegnano che spesso il criminale informatico è giovane, ben istruito e ben integrato nel proprio contesto sociale, a volte nemmeno realmente consapevole del reale disvalore della condotta posta in essere: un criminale “dal colletto bianco”, che commette questi illeciti più per sfida intellettuale, prestigio, e solo da ultimo specificamente per danneggiare gli utenti.

In questo contesto spicca la frode informatica, che per frequenza statistica ed entità dei danni economici arrecati è uno degli illeciti informatici più pericolosi: se solo si prova a digitare su un qualsiasi motore di ricerca “frode informatica” compaiono numerosissimi risultati di casi più o meno gravi all’ordine del giorno.

Essa consiste in un’aggressione al patrimonio altrui attraverso la “manipolazione” o “utilizzazione fraudolenta” di processi o sistemi automatizzati di elaborazione, trasmissione o trattamento di dati e informazioni.

L’intento di questo lavoro di ricerca è analizzare la genesi e la struttura della fattispecie di *frode informatica*, le sue intersezioni e i suoi collegamenti con disposizioni “limitrofe”, che sanzionano comportamenti simili dal punto di vista fattuale e non così diversi dal punto di vista giuridico, come l’*indebito utilizzo di una carta di pagamento magnetica*; particolare attenzione sarà data all’analisi della circostanza aggravante introdotta nel 2013 al comma terzo (frode informatica commessa con “sostituzione di identità digitale”) e alle problematiche che ad oggi più animano dottrina e giurisprudenza, sia di tipo processuale sia di tipo sostanziale, segnandone la tendenza evolutiva.

Successivamente ci si sofferma sulle strategie di tipo preventivo, citando alcuni interventi realizzati in Italia, in Europa e sul piano internazionale; nell’ultimo capitolo si vuole analizzare in una prospettiva comparata come l’ordinamento spagnolo ha affrontato il fenomeno, evidenziando le similitudini e le differenze con le scelte italiane. Infine le conclusioni cercano di sintetizzare le generali tendenze e fornire utili spunti de iure condendo ulteriori a quelli nei singoli capitoli, sia dal punto di vista della riformulazione della normativa esistente e dell’interpretazione sulla stessa sia dal punto di vista del necessario sforzo di tipo extrapenale e più propriamente informatico per un’azione efficace.

Capitolo I: Introduzione storica e genesi normativa

1.1 Le iniziative a livello internazionale e sovranazionale: OCSE, Consiglio d'Europa e Comunità Europea

L'introduzione della fattispecie di frode informatica nell'ordinamento giuridico italiano avviene nel 1993 con la legge n. 547, su impulso soprattutto degli organismi sovranazionali e internazionali cui l'Italia partecipa ed al fine di approntare una tutela giuridica organica ed adeguata di fronte alla diffusione crescente di illeciti legati alle nuove tecnologie.

Le organizzazioni internazionali iniziarono ad esaminare e studiare gli illeciti informatici negli anni '80: prima l'OCSE creò nel 1984 un gruppo di esperti che avrebbero dovuto studiare gli aspetti giuridici e socio-economici della frode informatica, analizzare gli orientamenti normativi e le soluzioni in concreto adottate, per poi fornire dei suggerimenti di politica legislativa (c.d. *soft-law*, comportamenti che tutti gli Stati membri avrebbero dovuto perseguire)[1]; poi nel 1985 il Consiglio d'Europa creò un Comitato ristretto di esperti con l'incarico di studiare il fenomeno della criminalità informatica e di preparare delle *linee guida* e dei *principi direttivi* utili per la redazione e l'armonizzazione delle leggi nazionali (questo studio funse poi da base delle due liste confluite nella Racc. n. 9/1989, su cui *infra*). La Comunità Europea iniziò ad interessarsi al "*problema informatico*" nel 1982, patrocinando due importanti ricerche sulla vulnerabilità dei sistemi informatici ormai diffusi in Europa e sugli effetti intersettoriali determinati dagli accessi abusivi e dalle frodi informatiche in senso lato[2]: furono i primi risultati a livello europeo con cui si evidenziavano le carenze dal punto di

[1] Il gruppo di esperti redasse un lungo rapporto in cui elencò una serie di comportamenti che dovevano costituire un denominatore comune da perseguire e sanzionare da parte di tutti i Paesi membri pur attraverso i differenti approcci: il primo era proprio la frode informatica "*con l'intenzione di commettere un trasferimento illegale di fondi o di altre cose di valore*".

[2] La prima ricerca si svolse fra il 1982 e il 1983 ed esaminò 115 casi di abusi informatici ed incidenti nel settore accaduti in Belgio, Francia, Italia, Regno Unito e Germania, concludendosi con la formulazione di una raccomandazione e di uno schema di azione di livello comunitario.
La seconda ricerca venne coordinata dall'ISTEV (Istituto per le Studio della Vulnerabilità delle Società Tecnologicamente Evolute, oggi abolito) e riguardava gli effetti derivanti dall'accesso illegittimo o dal cattivo funzionamento dei sistemi di computers e quale fosse il ruolo di questi ultimi apparecchi, utilizzati come supporto nelle attività di produzione di beni e servizi.

vista della sicurezza che acuivano i rischi di incidenti e di danni economici anche di rilevante entità derivanti dai *computer crimes*. Si sollecitavano quindi i pubblici poteri a farsi carico delle conseguenze derivanti dai predetti incidenti.

Nel 1988, durante la riunione dell'Osservatorio Giuridico della Commissione europea, vi fu vivo interesse per la criminalità informatica: si affermò che la Commissione UE avrebbe dovuto promuovere l'applicazione in tutti gli Stati membri dei principi direttivi che il Comitato del Consiglio d'Europa stava elaborando[3].

Nel 1988 terminò anche il lavoro del Comitato di esperti incaricato dal Consiglio d'Europa di studiare il problema della criminalità informatica: il gruppo elaborò due liste distinte di comportamenti, una "*minima*" e una "*facoltativa*".

Nella lista minima furono inserite quelle condotte che, a giudizio unanime del comitato, tutte le legislazioni penali nazionali avrebbero dovuto perseguire e sanzionare con l'arma della pena; nella lista facoltativa furono inseriti quei comportamenti che non avevano trovato il consenso unanime degli esperti sull'*an* o sul *quomodo* della tecnica sanzionatoria e che quindi potevano essere perseguiti e sanzionati a discrezione dei singoli Stati.

La frode informatica trovò collocazione nella lista minima: tutti gli esperti quindi concordavano sulla pericolosità di tale fattispecie e sulla necessità di repressione penale dei comportamenti consistenti nella "*introduzione, alterazione, cancellazione o soppressione di dati o programmi o in qualsiasi altro tipo di ingerenza in un procedimento di elaborazione di dati che, influenzandone il risultato, cagioni ad altri un pregiudizio economico e materiale, al fine di procurare a sé o ad altri un ingiusto profitto*"[4].

---

[3] Anche la Camera di Commercio Internazionale si interessò al problema informatico: nel 1988 pubblicò un rapporto intitolato "*Computer related crime and criminal law: an International Business View*" con cui si sosteneva con forza la necessità di un intervento penale per difendere i patrimoni di informazioni sempre più spesso sotto minaccia a causa degli accessi e dell'utilizzazione non autorizzata degli elaboratori e dei sistemi telematici. Si focalizzava l'attenzione anche sul carattere internazionale di tali fattispecie, che spesso acuisce il problema. Rivolse poi diverse raccomandazioni all'allora Comunità Economica Europea affinché vigilasse sull'azione degli Stati membri, di modo tale che questi fossero solerti nel prevedere e sanzionare in maniera effettiva gli illeciti informatici analizzati e vi fosse stretto coordinamento nella repressione sovranazionale.

[4] Nella lista minima trovarono collocazione: frode informatica, falso informatico, danneggiamento dei dati e dei programmi informatici, sabotaggio informatico, accesso non

Rispetto alle condotte inserite nella lista minima, la Raccomandazione del Consiglio d'Europa ha sollecitato una considerazione nuova da parte dei legislatori nazionali, anche nel caso in cui avessero già provveduto ad introdurre disposizioni apposite: si sottolineava così l'importanza di una politica legislativa uniforme nei diversi Paesi sia per evitare che la difficoltà di collaborazione internazionale sfociasse in impunità, sia per scongiurare i pericoli derivanti dall'esistenza di c.d. "paradisi informatici".
Nel 1994 arrivò sostanziale adesione alle linee di fondo del lavoro del Consiglio d'Europa da parte dell'*Assiociatión International de Droit Pénal*, la quale ha posto la criminalità informatica al centro del suo XV Congresso: in tale sede, si è suggerito di considerare le condotte di abuso dell'informatica in maniera unitaria e non in due liste separate e fu proposto di introdurre ulteriori fattispecie meritevoli di attenzione da parte del legislatore penale[5].

1.2 La Legge n. 547/1993: iter legislativo e problematiche connesse

Questo il panorama che portò alla promulgazione nel 1993 della legge n. 547 (recante "*Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*" in G.U. n. 305 del 30 dicembre 1993)[6] e al conseguente ammodernamento del nostro codice penale. Nell'iter legislativo la Commissione Ministeriale di esperti ha dovuto affrontare varie questioni[7].

---

autorizzato, riproduzione non autorizzata di un programma informatico protetto, riproduzione non autorizzata di una topografia informatica.
La lista facoltativa riguardava invece: alterazione dei dati o dei programmi informatici, spionaggio informatico, utilizzazione non autorizzata di un elaboratore, utilizzazione non autorizzata di un programma informatico protetto.

[5] Vedi ad esempio "Commercio di codici d'accesso ottenuti illecitamente" e "Diffusione di programmi virus o programmi similari".

[6] Prima della L. 574/1993 il legislatore italiano era intervenuto in maniera settoriale, regolando solo alcune specifiche ipotesi di illeciti *latu sensu* informatici. Nel 1978 con la l. n. 191 è stato introdotto nel codice penale l'art. 420 "Attentato ad impianti di pubblica utilità"; la l. n. 121 del 1980 disciplinò *Comportamenti illeciti in ambito di discipline extrapenali*; nel 1991 la l. n. 197 intervenne per la prima volta nei confronti *dell'Abuso di carte magnetiche di pagamento*; infine il d.lgs. n. 518/1992 in materia di Tutela *del software e topografie per prodotti semiconduttori*.

[7] Per l'elaborazione del progetto di legge, il Ministro della Giustizia dell'epoca, prof. Giuliano Vassalli, nominò una Commissione composta da magistrati, accademici ed esperti informatici. I

Primo problema fu scegliere se modificare il codice penale vigente o introdurre una legge speciale ad hoc: la scelta cadde sulla modifica del corpus codicistico introducendo i nuovi reati informatici accanto alle figure di reato ad essi più contigue dal punto di vista dell'oggetto giuridico, "*nella convinzione che la particolarità della materia non costituisse ragione sufficiente per la configurazione di uno specifico titolo*"[8]. Si volle rispettare la struttura codicistica scelta dal legislatore del 1930 ispirata dal criterio del bene giuridico tutelato, poiché si riteneva – con grande lungimiranza – che le diverse manifestazioni della criminalità informatica costituissero mere modalità particolari di aggressione di beni giuridici già individuati come meritevoli di tutela, peculiari solo per l'oggetto materiale[9].

Ulteriore profilo problematico riguardava la scelta dei comportamenti ai quali attribuire rilevanza penale[10]: la Commissione in primis ritenne di non poter limitare la previsione delle nuove fattispecie penali esclusivamente alla lista "minima" del Consiglio d'Europa. La repressione penale doveva interessare

---

lavori della Commissione iniziarono nel 1989 con una serie di audizioni, convocando i rappresentanti delle categorie più interessate del parastato nonché i rappresentanti delle maggiori associazioni imprenditoriali e professionali del settore bancario, assicurativo, industriale e delle più importanti associazioni di produttori di hardware e software. La Commissione terminò i suoi lavori nel 1991 ma il testo definitivo finì per rimanere dimenticato fra le carte del Gabinetto del Ministro. Solo verso le fine del 1992 fu riconsiderato dal Ministro della Giustizia, prof. Conso, il quale lo trasmise al Parlamento con l'approvazione del Consiglio dei Ministri.

[8] Così si sosteneva nella Relazione del Disegno di legge n. 2773 – *"Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica*", presentato dal Ministro di Grazia e Giustizia.

[9] A conferma del dibattito su questo aspetto, si segnala che in Parlamento fu presentato un disegno di legge che mirava ad introdurre nel Capo III del Titolo XII una nuova IV Sezione, dal titolo "*Dei delitti in materia informatica e telematica*" (Camera dei Deputati, XI Legislatura, n. 1174). Inoltre, all'interno della Commissione, il prof. Frosoni si dichiarò contrario all'impostazione scelta dalla maggioranza e riportò le sue critiche in un articolo dal titolo "*Il disegno di legge sulla repressione dei reati informatici*" pubblicato in *Informatica e Documentazione*, n. 4 del 1993, pag. 31 e segg.

[10] Si scelse di non fornire una definizione di delitto informatico, sia per ragioni di natura pratica, sia per ragioni di natura sistematica. In primis, il dibattito che sul tema si era sviluppato nei trent'anni precedenti non aveva portato a risultati tangibili dal punto di vista dell'omogeneità delle posizioni: si erano susseguite varie definizioni che spesso, per poter davvero essere generali, risultavano sostanzialmente vuote o meramente descrittive della situazione esistente. Inoltre è pericoloso cristallizzare in definizioni settori in continuo sviluppo come quelli tecnologici: il sistema avrebbe presto rischiato di basarsi su una definizione obsoleta. In secondo luogo, creare una speciale categoria di "beni informatici" con una definizione avrebbe causato distorsioni con la scelta del legislatore di aggiornare, per così dire, le singole disposizioni incriminatrici, rispettando la sistematica del codice basata sul criterio del "bene giuridico tutelato".

anche comportamenti individuati nella lista "facoltativa", sui quali tuttavia si svolse un acceso dibattito rispetto al tipo di sanzione (amministrativo/penale) adeguata.

Le frodi informatiche furono uno dei primi e più importanti settori in cui intervenne la legge n. 547/1993: l'intervento si riteneva necessario poiché le stesse si caratterizzavano per il fatto di essere realizzate attraverso lo strumento informatico, senza quindi ricorrere l'induzione in errore di un essere umano[11]. L'attenzione si focalizzava sulle manipolazioni di dati, attraverso le quali è possibile interferire abusivamente nel funzionamento di un elaboratore elettronico e procurarsi così un illecito arricchimento con altrui danno, senza coinvolgere direttamente un soggetto "vittima".

Il legislatore del 1993 ritenne quindi indispensabile l'introduzione di una fattispecie ad hoc poiché si trattava di condotte non appartenenti al novero di quelle già dotate di rilevanza penale in base alle norme vigenti.

Tali condotte si avvicinavano concettualmente alla truffa senza però integrarne tutti i requisiti tipici; si avvicinavano anche a fattispecie lesive del patrimonio come il furto, senza però che vi fosse una cosa a pieno titolo materiale suscettibile di apprensione e sottrazione[12].

Per combattere queste forme di impiego fraudolento della nuova tecnologia è stata inserita nel codice penale la nuova fattispecie di frode informatica. L'art. 10 della l. 547/93 ha introdotto l'art. 640-*ter* c.p., rubricato *Frode informatica* che dispone quanto segue: *"chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 516 a euro 1.032. La pena è della reclusione da uno a cinque anni e della*

[11] Parte della dottrina ritiene tutt'oggi che vi sia comunque un'induzione in errore del soggetto che predispone in un certo modo un sistema informatico e che si ritrova quindi ad essere ingannato a causa dei comandi abusivi impartiti dall'agente (sul punto vedi *infra* cap. II).

[12] In Commissione vi fu un acceso dibattito sul concetto di bene informatico e quindi sulla natura dei dati e dei programmi informatici. Prevalse la linea della maggioranza che riteneva non potessero essere considerati beni in senso stretto dato che i dati e i programmi si sostanziano in informazioni e l'informazione non ha una propria materialità: al più può essere conosciuta e non posseduta.

multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal n. 1 del secondo comma dell'art. 640 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema. […]" , il cui modello fu senz'altro la fattispecie tradizionale di truffa, come sottolinea la Relazione governativa al progetto di legge[13]; incriminazione che tuttavia difficilmente risultava applicabile in un contesto informatico.

Da più parti si è rilevato che sarebbe stata più consona la denominazione di "*truffa informatica*", considerando che l'espressione "frode" è un termine ambiguo, utilizzato in maniera promiscua sia dal legislatore sia dalla dottrina. Probabilmente la scelta del legislatore di utilizzare il termine "frode" anziché quello di "truffa" fu dettata dall'intento di sottolineare contemporaneamente la differenza strutturale e la vicinanza concettuale fra le fattispecie: le due norme sono diverse solo per il fatto (non marginale) che l'una, la truffa, rimane sempre una fattispecie bilaterale necessaria, l'altra, la frode, non implica necessariamente un rapporto con un altro soggetto-persona fisica né a maggior ragione un'induzione in errore di "taluno", conservando tuttavia un'attitudine fraudolenta. Giorgio Pica fu il primo a rilevare come sia possibile individuare un minimo comune denominatore delle molte e poliedriche ipotesi di "frode" esistenti nella legislazione penale, vale a dire l'"*oggettiva idoneità ingannevole della condotta*"; le finalità soggettive, le concrete modalità d'azione e la situazione psicologica del soggetto passivo sono solo occasionali "variabili" inserite dal legislatore in funzione della *species* di fatti da incriminare. In tal modo al concetto di "frode" è riconosciuta una valenza di *genus* che la rende di universale applicabilità: gli ulteriori elementi rappresentano meri elementi caratteristici di singole ipotesi[14].

La legge 547/1993 non si occupò del problema della rilevanza penale di quell'altra forma di frode informatica che si sostanzia nell'utilizzo indebito di una carta di debito o di credito sia come strumento di prelievo di denaro contante sia

---

[13] "*Per la nuova ipotesi, che al pari della truffa è collocata nel capo II del c.p. le nozioni di ingiustizia del danno e di altruità sono mutuabili dall'affine fattispecie di cui all'art. 640 c.p. della quale riproduce altresì il regime di procedibilità ed il profilo sanzionatorio*", così la Relazione governativa in *Diritto dell'informazione e informatica*, 1992, p. 633 (comunque più diffusamente *infra* cap. II)

[14] G. Pica, *Diritto penale delle tecnologie informatiche*, UTET, Torino, 1999

come mezzo di pagamento negli esercizi commerciali: questo fenomeno non era considerato sostanzialmente informatico poiché si concepiva frode informatica solo quella che aveva di mira un elaboratore elettronico inteso come Personal Computer fisico o come sistema complesso; quindi la condotta di colui che si appropria di denaro altrui attraverso l'indebito utilizzo di una carta di debito o di pagamento o "striscia" senza facoltà legittima una carta di pagamento altrui per fare acquisti nulla aveva a che fare con il mondo dell'informatica.

Tali condotte sono diventate penalmente rilevanti con un altro intervento legislativo ad hoc, predisposto per fronteggiare il riciclaggio di denaro "sporco" , la L. n. 197/1991: veniva valorizzata soprattutto la funzione di strumento di pagamento alternativo al denaro contante che le carte di debito e di pagamento possiedono. Da ultimo questa fattispecie è confluita nel D.lgs. n. 231/2007 (art. 55 c. IX) di "*Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione.*"

1.3 La Ratifica della *Convenzione "Cybercrime"*

Nel 2008, mentre Internet diventava sempre più un fenomeno globale, la Commissione interministeriale composta dai Ministri D'Alema, Mastella, Gentiloni e Nicolais ha presentato il disegno di legge[15] con cui si ratificava sul finire della legislatura la Convenzione *"Cybercrime*" del Consiglio d'Europa firmata a Budapest nel 2001[16].

Nel disegno di legge e nei lavori preparatori è stato sottolineato più volte come l'Italia sia stato uno dei primi Paesi europei a dotarsi nel '93 di una legge organica in materia di illeciti informatici; l'intervento per l'esecuzione della

[15] Disegno di legge n. 2807 del 19 giugno 2007

[16] La legge n. 48, recante "*Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica e norme di adeguamento dell'ordinamento interno*", introduceva nell'ordinamento gli obblighi sottoscritti dall'Italia a Budapest il 23 novembre 2001. La legge fu approvata dal Senato il 27 febbraio 2008 e quindi pubblicata in G.U. il 4 aprile 2008 n. 80, entrando in vigore il giorno successivo.

Convenzione “Cybercrime” è risultato dunque nei fatti modesto, essendo già in vigore una disciplina sotto molti aspetti esaustiva.

Forse proprio questa convinzione ha creato le premesse per un iter parlamentare estremamente rapido e su certi aspetti poco attento, dato che sono state approvate disposizioni con formulazioni delle cui incongruenze i parlamentari stessi si sono resi conto (auspicando l’intervento correttivo della giurisprudenza) e sono state inserite fattispecie nuove che non sono affatto esecutive rispetto alla Convezione, a dispetto del dichiarato intento di “*consentire l’adeguamento dell’ordinamento italiano alla normativa internazionale*”.

Il delitto di frode informatica non ha subito particolari modificazioni nella sua formulazione: si riteneva infatti di aver già adempiuto agli obblighi internazionali con la formulazione del 1993. Anzi, la formulazione codicistica, richiedendo il mero dolo generico[17], sanziona una più ampia sfera di condotte dannose persino rispetto all’art. 8 della Convenzione[18], il quale, stabilendo che la condotta deve essere posta in essere “intenzionalmente” richiede – secondo molti – il dolo specifico.

Fra le disposizioni della l. n. 48/2008 che non sono affatto esecutive di obblighi internazionali, rispondendo piuttosto ad autonome scelte del legislatore italiano di incriminare specifiche condotte, spicca l’inserimento nel codice penale del’art. 640-*quinquies* c.p. che punisce la “*frode informatica del soggetto che presta servizi di certificazione di firma elettronica*”.

Si tratta di un nuovo reato proprio del fornitore di servizi di certificazione di firma elettronica, configurato – nelle intenzioni della Relazione di accompagnamento – come una nuova *species* di truffa, che sanziona penalmente la violazione degli obblighi previsti dalla legge per il rilascio di un certificato qualificato,

[17] Il punto non è pacifico in dottrina: parte minoritaria ritiene che sia richiesto il dolo specifico. Sul punto vedi *infra* cap. II.

[18] Articolo 8 della Convenzione di Budapest, rubricato *Frode informatica*, stabilisce quanto segue: “*Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale, se commesso intenzionalmente e senza alcun diritto, il cagionare un danno patrimoniale ad altra persona:*
a. con ogni introduzione, alterazione, cancellazione o soppressione di dati informatici;
b. con ogni interferenza nel funzionamento di un sistema informatico, con l’intento fraudolento o illegale di procurare, senza alcun diritto, un beneficio economico per se stesso o altri.”

allorquando sussiste altresì il fine di procurare per sé o altri un ingiusto profitto con altrui danno[19].

I primi commentatori hanno sottolineato principalmente l'opportunità di tale intervento additivo, stante la maggiore carica offensiva della condotta posta in essere dal certificatore e dal ruolo svolto[20].

Molta parte della dottrina però è critica verso l'introduzione delle cc.dd. norme penali "in bianco", prescrizioni prive di un proprio contenuto precettivo e meramente sanzionatorie di condotte illecite previste in sede extrapenale: nel caso in esame, infatti, la maggior parte degli obblighi è prevista all'art. 32 commi 2 e segg. del Codice dell'amministrazione digitale[21]. All'art. 640-quinquies c.p. è estraneo qualsiasi requisito intrinseco di "fraudolenza", che dovrebbe invece caratterizzare le fattispecie di frode.

La Convenzione *Cybercrime*, infine, è intervenuta sulla responsabilità derivante da reato delle persone giuridiche, estendendola a tutte le fattispecie in essa contemplate[22].

---

[19] La necessità di tale fattispecie deriva dal rilievo che non sarebbe stata sufficiente la fattispecie di frode informatica, poiché spesso nell'attività del certificatore potrebbero non sostanziarsi le condotte di "alterazione nel funzionamento di un sistema" o di "intervento senza diritto su dati, informazioni o programmi". Il certificatore è per definizione un soggetto che agisce "con diritto" sul sistema e le sue operazioni permettono al sistema di funzionare.
Tale considerazione "meramente negativa" secondo L. Picotti non giustifica comunque la creazione, denominazione e collocazione del nuovo delitto quale ipotesi qualificata di truffa. Vedi L. Picotti, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Diritto penale e processo*, 2008, n. 6

[20] Vedi fra tutti Articolo di M. Cuniberti, G.B. Gallus, F.P. Micozzi, S. Aterno, "*Cybercrimine: prime note sulla legge di ratifica della Convenzione di Budapest*", del 08/05/2008 su Altalex, http://www.altalex.com/index.php?idnot=41438

[21] Il medesimo Codice già sanzionava civilmente la violazione di tali obblighi da parte del certificatore accreditato all'art. 30 c. 1 lett. d)

[22] L'articolo 12 della Convenzione, rubricato "*Responsabilità delle Persone Giuridiche*" stabilisce: *1. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie affinché le persone giuridiche possano essere ritenute responsabili di un reato in base a questa Convenzione commesso per loro conto da una persona fisica che agisca sia individualmente che come membro di un organo di una persona giuridica che eserciti un potere di direzione al suo interno, nei termini che seguono:*
a. un potere di rappresentanza della persona giuridica;
b. un'autorità per assumere decisioni nel nome della persona giuridica;
c. un'autorità per esercitare un controllo all'interno della persona giuridica.
2. In aggiunta ai casi già previsti nel paragrafo 1. di questo articolo, ogni Parte deve adottare le misure necessarie affinché una persona giuridica possa essere ritenuta responsabile se la mancanza di sorveglianza o controllo di una persona fisica di cui al paragrafo 1. ha reso possibile la commissione di reati previsti al paragrafo 1. per conto della persona giuridica da parte di una persona fisica che agisca sotto la sua autorità.
3. Secondo i principi giuridici della Parte, la responsabilità delle persone giuridiche può essere penale, civile o amministrativa.

La legge di ratifica ha introdotto un nuovo art. 24-bis nel d.lgs. 231/2001 che estende ai reati informatici previsti con la stessa novella la responsabilità da reato degli enti, facendo salvo però "*quanto previsto dall'articolo 24 del decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico*". Ciò ha comportato l'anomala esclusione del delitto di frode informatica di cui all'art. 640-ter comma 1 c.p. dalle ipotesi di responsabilità da reato degli enti, quando non sia commesso in danno dei soggetti pubblici sopra citati. L'esclusione è apparsa fin da subito anomala ed irragionevole, dato che in astratto è perfettamente ipotizzabile la commissione di un delitto di frode informatica da parte di un soggetto interno ad un'impresa con conseguente danno patrimoniale ingente, a prescindere dal coinvolgimento dell'erario statale. Si veniva a creare una disparità di trattamento difficilmente giustificabile sul piano della razionalità costituzionale. Inoltre si creavano frizioni con la disciplina internazionale, dato che la disposizione convenzionale era chiara nel prevedere l'obbligo per ogni Stato di introdurre una responsabilità da reato (amministrativa o penale) per gli enti anche nel caso di frode informatica; non prevedeva alcuna differenziazione fra ipotesi in danno di un ente pubblico ovvero ipotesi di danno "privatistico".

Infine non era contemplata una responsabilità amministrativa da reato neppure con riguardo alla fattispecie "contigua" di indebito utilizzo, falsificazione, alterazione di carte di credito o di pagamento, ovvero di qualsiasi altro documento analogo prevista all'art. 55 c. IX del d.lgs. n. 231/2007: come se anche tale fattispecie non potesse essere posta in essere con il coinvolgimento a vario livello di un ente e non potesse essere fortemente dannosa sia per i soggetti privati sia per l'ente stesso[23].

Questo difetto di coordinamento è stato parzialmente sanato nel 2013 con il decreto-legge n. 93, che a distanza di pochi anni ha modificato l'art. 24-bis del d.lgs. n. 231/2001: sono state così aggiunti fra le fattispecie di reato presupposto di responsabilità dell'ente il caso di cui all'art. 55 c. IX e quello di

---

4. Questa responsabilità è stabilita senza pregiudizio per la responsabilità penale delle persone fisiche che hanno commesso il reato.

[23] Si ritiene importante sottolineare come la disposizione di cui all'art. 55 è stata introdotta nell'ambito di un intervento normativo finalizzato ad arginare il fenomeno del riciclaggio di denaro "sporco", in primis posto in essere –insegna la criminologia- attraverso le persone giuridiche. Il fatto che non fosse prevista una responsabilità da reato dell'ente lasciava preoccupanti zone d'impunità nell'ordinamento.

frode informatica commessa con sostituzione d'identità digitale, ipotesi inserita ex novo da tale decreto al comma 3 dell'art. 640-ter c.p..

Si rileva la parzialità dell'intervento, poiché permane l'opinabile esclusione dell'ipotesi base di frode informatica dal novero dei reati presupposto della responsabilità dell'ente.

Con la ratifica della convenzione "*Cybercrime*", infine, il legislatore è intervenuto anche sul codice di procedura penale, inserendo disposizioni relative alla comunicazione rapida dei dati immagazzinati, la raccolta dei dati di traffico in tempo reale, le ispezioni, le perquisizioni, le intercettazioni e il sequestro di dati informatici: sono state così positivizzate alcune prassi consolidate in tema di investigazioni informatica[24].

L'impostazione finalistica di tali integrazioni, focalizzata sull'obiettivo perseguito più che sul metodo utilizzato in concreto nelle indagini, permette di adeguare in via di fatto le disposizioni processuali agli sviluppi della tecnica informatica, evitando la cristallizzazione di modalità operative presumibilmente presto obsolete e sempre migliorabili.

1.4 Recenti modificazioni

L'ultimo intervento in materia di frode informatica si è avuto nel 2013 con il decreto-legge n. 93, provvedimento alquanto eterogeneo[25] che ha inserito un nuovo comma terzo all'art. 640-ter c.p.: "*La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.*"

Si è trattato di un intervento variegato (un c.d. "decreto omnibus"), con cui il legislatore ha tentato di dare una pronta risposta ad una moltitudine di

[24] Si è voluto introdurre una disciplina attenta in primo luogo al risultato della ricerca probatoria, volta alla tutela dell'integrità dei dati informatici durante la ricerca: è stata prevista infatti "*l'adozione di misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, e in altri casi l'adozione di procedure che assicurino la conformità dei dati acquisiti a quelli originali e la loro immodificabilità*"

[25] D.lg. 14 agosto 2013, n. 93 "*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*." In *G.U. serie generale n. 191 del 16/8/2013* (più conosciuto come Decreto sul c.d. Femminicidio)

problematiche percepite dalla collettività come contingenti e meritevoli di attenzione. Una di queste è il furto di dati sensibili via Internet, al fine di realizzare un profitto personale con altrui danno; la Relazione al Parlamento del disegno di legge infatti ha individuato la *ratio* di questa innovazione normativa nel "*rendere più efficace il contrasto del preoccupante e crescente fenomeno del cosiddetto «furto d'identità digitale», attraverso il quale vengono commesse frodi informatiche, talora con notevole nocumento economico per la vittima*"[26].

Il vuoto legislativo rispetto a questo fenomeno era stato denunciato da più parti[27], sia nell'apparato interno statale sia a livello sovranazionale, anche considerando la sempre maggior diffusione dell'utilizzo dei social network che erano totalmente sconosciuti al legislatore del 1993 e poco noti a quello del 2008.

La frettolosità dei lavori però ha lasciato irrisolti vari dubbi, sui quali si vorrà riflettere più diffusamente.

[26] Relazione alla Camera dei Deputati di presentazione del Disegno di Legge n. 1540 di conversione del decreto-legge 14 agosto 2013, n. 93, presentato il 16 agosto 2013, http://www.camera.it/leg17/995?sezione=documenti&tipoDoc=lavori_testo_pdl&idLegislatura=17&codice=17PDL0009030&back_to=http://www.camera.it/leg17/126?tab=2-e-leg=17-e-idDocumento=1540-e-sede=-e-tipo=

[27] Si veda la Comunicazione della Commissione Europea "*Verso una politica generale di lotta contro la cybercriminalità*" (COM (2007) 267), dove si legge: "*Il furto di identità in quanto tale non costituisce fattispecie di reato in tutti gli Stati membri. Poiché però è spesso più facile provare il reato di furto di identità che quello di frode, la cooperazione fra le autorità di contrasto dell'UE sarebbe agevolata se tutti gli Stati membri considerassero reato il furto di identità"*. La IX Commissione della Camera dei Deputati (DOC XVII, n. 26 del 22/01/2013) ha sostenuto che "*per combattere efficacemente il furto d'identità digitale, oltre alle misure di carattere preventivo […], appare necessario dotare le istituzioni di adeguati strumenti normativi, introducendo nell'ordinamento il reato di furto d'identità digitale, prevedendo adeguate sanzioni penali*".

Capitolo II: Analisi della struttura del delitto di frode informatica

2.1 Il bene giuridico tutelato

Il delitto di frode informatica è stato collocato nel nostro codice penale subito dopo il delitto di truffa (art. 640 c.p.), a sottolineare la contiguità concettuale e giuridica delle due fattispecie. Già si è detto, infatti, che la *ratio* ispiratrice dell'innovazione legislativa era l'impossibilità di applicare la fattispecie tradizionale di truffa alle condotte realizzate attraverso un elaboratore elettronico. A più di vent'anni dalla sua introduzione, dottrina e giurisprudenza rimangono divise rispetto al considerare la disposizione del 1993 semplicemente come una truffa che avviene in ambito informatico: vi sono elementi peculiari dell'una e dell'altra disposizione, tanto che parte della giurisprudenza ritiene configurabile il concorso[1]. Per capire se la fattispecie prevista all'art. 640-ter c.p. sia un'ipotesi speciale rispetto al reato di truffa oppure se costituisca un'autonoma fattispecie delittuosa, è necessario condurre un'analisi comparativa delle due norme volta ad evidenziare gli elementi differenziali così come quelli comuni tra le due fattispecie.

Primo aspetto da analizzare è quello relativo al bene giuridico tutelato: ci si deve chiedere quale sia l'interesse meritevole di tutela in base al quale il legislatore ha ritenuto opportuno intervenire con un precetto penale.

La collocazione sistematica, la struttura della fattispecie e, seppur con cautela, la rubrica della stessa hanno portato la dottrina maggioritaria a sostenere che il delitto di frode informatica sia stato posto a tutela del patrimonio[2].

In primis è importante il dato sistematico: la fattispecie è stata collocata nel Titolo XIII del Libro II del codice penale dedicato ai "*Delitti contro il patrimonio*", subito dopo la fattispecie tradizionale di truffa, paradigmatica fra i delitti commessi "mediante frode"[3].

---

[1] Sul punto più diffusamente *infra*

[2] G. Pica, "*Diritto penale delle tecnologie informatiche*", UTET, 1999; S. Logroscino, "*La frode informatica quale autonoma figura di reato rispetto al delitto di truffa*", 21/12/2011, reperibile su Altalex: http://www.altalex.com/index.php?idnot=16607

[3] Art. 640 c.p., "Truffa", stabilisce: *"Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.*

Anche l'analisi della struttura della fattispecie dà prova dell'interesse tutelato: si tratta di un puro reato di danno, costruito sul binomio condotta-evento, il cui momento consumativo si concretizza nell'illecito profitto per sé o per altri con altrui danno (entrambi connotati patrimonialmente). Come si avrà modo di approfondire, lo sviluppo causale è simmetrico a quello che già caratterizza la truffa, della quale perciò condivide l'oggetto giuridico. Prima della verificazione dell'evento-danno, il reato non può sussistere, non essendo integrato un elemento tipico della fattispecie; inoltre, a ben vedere, la valorizzazione del principio di economicità processuale rende evidente come le lesioni al regolare funzionamento del sistema in quanto tale o alla riservatezza trovino presidio attraverso altre fattispecie[4]. Pur essendo tipizzate le modalità della condotta che hanno rilevanza penale[5], non si tratta di un reato di mera condotta, quindi non può condividersi quell'orientamento, pur degno di nota, che individua il bene giuridico tutelato nella riservatezza nel legittimo utilizzo dei sistemi informatici e telematici o nel regolare funzionamento del sistema[6].

Manca nella disposizione il riferimento a qualsivoglia fenomeno psicologico o di induzione in errore di taluno: per questo l'interesse tutelato può ritenersi squisitamente patrimoniale e assume un significato esclusivamente economico che afferisce all'integrità del patrimonio aggredito dal soggetto agente[7].

Il patrimonio non va più inteso in una accezione statica come imputazione personale di ricchezza e di beni dotati di corporeità, ma va piuttosto concepito in una prospettiva dinamica, come insieme di situazioni giuridiche di cui è

La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549:
1) se il fatto è commesso a danno dello Stato o di un altro ente pubblico o col pretesto di far esonerare taluno dal servizio militare;
2) se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'Autorità.
Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal capoverso precedente o un'altra circostanza aggravante."

[4] Il riferimento corre in primis alle fattispecie di danneggiamento informatico e accesso abusivo al sistema informatico nonché al micro-sistema costruito con il d.lgs. n. 196/2003 in materia di tutela dei dati personali.

[5] C. Pecorella sottolinea la differenza sostanziale fra la fattispecie di truffa e quella di frode informatica: nell'un caso si ha una fattispecie a forma libera, nell'altro la tipizzazione delle condotte limita fortemente la portata applicativa. L'Autrice però non mette in dubbio l'oggettività giuridica della seconda fattispecie: più diffusamente *infra*.

[6] A. Masi sostiene che l'oggetto della tutela nel delitto ex art. 640-ter c.p. sia la libertà negoziale: A. Masi, "Frodi informatiche e attività bancaria" in Rivista penale dell'economia, 1995.

[7] Cecilia Del Re, "*La frode informatica*", Edizioni Polistampa, 2009.

titolare un soggetto e che possono trascendere la sfera della sua persona, concretizzandosi in attività, investimenti e risparmi anche indirettamente imputabili[8]. Infine, la rubrica dell'art. 640-ter c.p. fa un esplicito riferimento alla "frode", elemento caratterizzante ogni azione *ex se* idonea ad ingannare[9]; e il delitto in cui "gli artifizi e raggiri" idonei ad ingannare sono tratto qualificante è proprio la truffa, senza dubbio fattispecie posta a presidio del patrimonio.

Queste considerazioni di carattere per lo più dogmatico e formale non hanno trovato il consenso di altra parte della dottrina che, fin dall'emanazione della legge del 1993, si è interrogata sull'esistenza nell'ordinamento di un nuovo "bene informatico" o addirittura di "beni informatici" con riferimento all'oggetto di tutela della nuova normativa[10]. Le posizioni però non sono state omogenee sia per l'ontologica complessità della definizione del concetto di "bene" sia per la rilevanza da attribuire ad esso, anche nel senso di una sua eventuale pluralità.

Innanzitutto non vi era accordo fra chi riteneva che bene informatico fosse l'oggetto materiale del comportamento illecito[11] e chi riteneva invece costituisse un nuovo oggetto giuridico, interesse emergente che aveva ispirato l'intervento normativo del 1993[12]. Fra costoro però le soluzioni proposte erano diversificate: Militello individuava un nuovo unico bene giuridico, l'"intangibilità informatica", oggetto generale e omnicomprensivo della tutela[13]; Sieber identificava

---

[8] V. S. Moccia, "*Tutela penale del patrimonio e principi costituzionali*", Cedam, Padova, 1998 e C. Castronovo, a cura di, "*Manuale di diritto privato europeo, Volume 2*", Giuffrè Editore, 2007.

[9] G. Pica svolge un'attenta analisi sul concetto di "frode", partendo dal dato fattuale consistente nella varietà di situazioni giuridiche a cui il legislatore riferisce tale termine. Alcune fattispecie contemplano quale elemento del fatto soltanto il fine di ingannare, altre richiedono espressamente l'uso di artifici e raggiri e l'effettiva induzione in errore di taluno; altre prescindono del tutto da qualsiasi raggiro e dalla situazione psicologica della vittima. L'unica soluzione prospettabile per creare un concetto di "frode" coerente e di universale applicabilità è quella di riconoscervi il mero significato di "*idoneità oggettivamente ingannevole dell'azione*". Così G. Pica, "Diritto penale delle tecnologie informatiche", UTET, 1999

[10] V. Frosini, "*Informatica, diritto e società*", Giuffré, Milano, 1992; D. Fondaroli, "*La tutela penale dei beni informatici*", in Diritto dell'informazione e dell'informatica, 1996, 296; F. Berghella – R. Blaiotta, "*Diritto penale dell'informatica e beni giuridici*", in Cassazione penale, 1995.

[11] F. Berghella – R. Blaiotta, "*Diritto penale dell'informatica e beni giuridici*", in Cassazione penale, 1995, 2335.

[12] V. Frosini, Telematica, "*Informatica, diritto e società*", Milano, 1992, p. 64; V. Militello, "*Nuove esigenze di tutela penale e trattamento elettronico delle informazioni*", in Rivista trimestrale di diritto penale dell'economia, 1992, p. 373-374

[13] L'intangibilità informatica viene definita come "*l'esigenza di non alterare la relazione triadica fra dato della realtà, rispettiva informazione, e soggetti legittimati ad elaborare quest'ultima nelle sue diverse fasi (creazione, trasferimento, ricezione)*". Essa ha il pregio di cogliere un aspetto

nell'ambito dei singoli reati informatici, differenti e specifici beni giuridici, quale il bene dell'informazione[14].

Vi sono stati anche Autori che si sono spinti a configurare il bene informatico come "bene immateriale" con carattere di diritto reale: il diritto inerisce al bene che ne rappresenta l'oggetto, *ius in re propria*[15].

Sicuramente le nuove tecnologie informatiche, penetrando in ogni settore delle attività umane, hanno aperto nuovi orizzonti d'interesse in ambito scientifico e hanno stimolato nuovi dibattiti: spesso però lo studioso del diritto non si confronta con veri e propri nuovi beni giuridici. Se è vero che la Rete ha creato nuovi diritti, è altrettanto vero che principalmente si sono sviluppate nuove modalità di esercizio di diritti e facoltà già considerati meritevoli di tutela, rese possibili proprio dal progresso tecnologico. In questo senso, i sistemi informatici e telematici permettono nuove modalità di azione, lecite ed illecite. La Rete si configura semplicemente come un luogo nuovo, una diversa dimensione dematerializzata e globale (*Cyberspace*): in essa ogni individuo ha la possibilità di esercitare i diritti e le facoltà che l'ordinamento gli riconosce in quanto tale o può anche porre in essere attività illecite, così come accade in qualsivoglia luogo fisico.

Le aggressioni illecite che vengono perpetrate in un sistema informatico o telematico hanno come obiettivo principale la lesione di diritti personali e patrimoniali[16]. Di regola, non si differenziano dal punto di vista dell'offensività

---

comune della ratio di tutela delle fattispecie informatiche: l'esigenza di assicurare e proteggere la genuinità dei processi di elaborazione di dati e programmi.

[14] U. Sieber, "La tutela penale dell'informazione", in Rivista trimestrale di diritto penale dell'economia, 1992, p. 492.

[15] V. Frosini, *Introduzione*, "*Informatica, diritto e società*", Milano, 1992. L'Autore sottolinea spesso nei suoi scritti la differenza fra il bene-informazione, consistente nel dato informativo riferito ad un determinato soggetto, e il nuovo bene informatico, che si riferisce all'informazione sottoposta a trattamento automatizzato da parte dell'elaboratore. Egli ravvisa "l'essenza dell'informatica" nel trattamento elettronico di informazioni. Di qui ne deriva una nuova situazione giuridica soggettiva che inerisce direttamente al dato informatico. G. Pica confuta tale conclusione, sostenendo in primo luogo che non è possibile ridurre l'informatica alla sola elaborazione automatizzata di informazioni; sottolinea poi come, se anche si considerasse l'informazione automatizzata il bene giuridico di riferimento, essa potrebbe costituire l'oggetto di tutela solamente delle fattispecie in cui l'azione è finalizzata all'accesso illegittimo ad essa. Non sarebbe possibile spiegare in questi termini le fattispecie in cui l'informazione automatizzata è solo il mezzo per la commissione del fatto di reato.

[16] Il *computer crime* infatti può consistere in una nuova modalità di lesione di beni giuridici già tutelati dall'ordinamento o nella lesione di nuovi beni giuridici nati con lo sviluppo delle nuove tecnologie, come la tutela del domicilio informatico (che non ha nulla a che vedere con il

intrinseca della condotta: la peculiarità è il contesto, particolarmente favorevole al criminale per le caratteristiche prima evidenziate (anonimato, assenza di confini, difficoltà della persecuzione e repressione delle condotte, facilità d'azione con enormi possibilità di guadagno).

Individuare come bene giuridico unitario l'"*intangibilità informatica*" coglie un solo aspetto, generico, della ratio di tutela delle nuove tecnologie e tralascia i profili più sostanziali della lesione. Inoltre comporta il rischio di creare un categoria concettuale inutile dal punto di vista pratico e fuorviante anche rispetto alla scelta legislativa di distribuire le nuove fattispecie all'interno del codice penale vigente, rispettando la sistematica dei beni giuridici già individuati. Anche la ricostruzione del bene giuridico informatico come bene immateriale pare difficilmente condivisibile, sia perché le definizioni di bene immateriale susseguitesi in dottrina paiono poco adattabili al contesto informatico[17], sia per il fatto che le nuove tecnologie hanno una chiara ed innegabile materialità e fisicità. I dati vengono immessi nel sistema attraverso la digitazione di comandi tradotti in codice binario e memorizzati con micro - registrazioni magnetiche od ottiche (nel caso di CD-ROM). È vero che la tecnologia si sta sviluppando nella direzione della totale dematerializzazione dei contenuti del *cyberspace*[18], ma è altrettanto vero che permane la necessità di un intervento umano che immetta un *input* in un sistema informatico (spesso un server reale ad alta affidabilità collocato presso un fornitore di servizi), il quale poi si sostanzi in dati, informazioni, files e risorse utilizzabili dai clienti.

L'analisi deve essere condotta nei termini ordinari, senza farsi condizionare in qualche modo dalla componente informatica delle fattispecie e quindi enucleando da ciascuna il bene giuridico tutelato: potrà trattarsi di un nuovo bene oppure coincidere con un interesse già tutelato, come nel caso della frode informatica.

---

domicilio fisico ma è da considerarsi una proiezione della persona in ambito virtuale). Questi ultimi sono la minor parte ma negli ultimi anni stanno crescendo. G. Pica, *op.cit*; C. Pecorella, "Diritto penale dell'informatica", Cedam, 2006

[17] A. Torrente, P. Schlesinger, in "*Manuale di diritto privato*", Giuffré Editore, Milano, 2009 forniscono un'elencazione di beni immateriali: i diritti quando possono formare oggetto di negoziazione, gli strumenti finanziari dematerializzati, i dati personali, le opere dell'ingegno, la proprietà industriale. È evidente come non si possano assimilare dati, programmi e risorse online a tali tipologie di beni. In senso critico anche F. Berghella – R. Blaiotta, op. cit., 2336

[18] *E-commerce* e *bitcoin, server online, cloud computing*, per fare alcuni esempi.

Una precisazione appare opportuna: tutelare lo stesso oggetto giuridico non significa necessariamente che una norma sia *species* dell'altra. In altre parole, sostenere che il delitto di frode informatica è posto a tutela del patrimonio non implica di necessità che si avvalli la configurazione di detta fattispecie come mera specificazione in ambito informatico della più generale fattispecie di truffa.
Tale posizione, espressa fra tutti sul finire degli anni '90 da G. Pica[19], rispecchiava lo sviluppo informatico-tecnologico coevo e dà la misura sia della novità del fenomeno informatico sia della difficoltà di un suo corretto inquadramento giuridico; alla fine degli anni '90, l'uso di sistemi informatici e la creazione di una realtà virtuale erano agli albori, non erano ancora un fenomeno di massa. Allora si identificava il sistema informatico con il PC e il sistema telematico con più PC collegati, i micro-processori erano ancora lontani. I *personal computer* venivano utilizzati per lo più nel mondo del lavoro e della ricerca accademica come veri e propri strumenti, in grado di facilitare e migliorare notevolmente il lavoro "reale"; non avevano ancora le funzioni quotidiane, "domestiche" che hanno oggi e soprattutto non erano considerati porte d'accesso ad una dimensione "altra". Quindi difficilmente poteva concepirsi una frode che si sviluppasse totalmente in ambito informatico con caratteristiche sue proprie, completamente avulsa dalla struttura del reato di truffa e aliena da qualsiasi sostrato materiale.
L'approccio di Claudia Pecorella, che scrive fra il 2004-2006, è già diverso: l'Autrice, forse intravedendo le straordinarie potenzialità dell'I.C.T., sostiene sì che la fattispecie di frode informatica si ispira allo schema della truffa, ma presenta caratteristiche del tutto peculiari che la allontanano dalla figura-modello[20]. Ad ogni modo ciò non intacca l'oggettività giuridica, che rimane pur sempre la tutela del patrimonio.
Guardando alla concretezza delle relazioni giuridiche e cercando di evitare inutili quanto fuorvianti concettualizzazioni astratte, si può concludere che il bene giuridico tutelato dal delitto di frode informatica sia il patrimonio, seppur in

[19] L'Autore sosteneva che il bene giuridico tutelato dal reato di frode informatica fosse identico a quello del reato di truffa (v. *op.cit*.); in tal senso anche F. Mantovani, "*Diritto penale, Parte speciale, delitti contro il patrimonio*", Cedam, Padova, 2002.
[20] C. Pecorella, *op.cit*.

un'accezione nuova e più ampia di quella tradizionale.

Probabilmente non è l'unico, ma ciò non significa includere la fattispecie in esame nel novero dei reati plurioffensivi, come autorevole dottrina[21] ha sostenuto: numerosissime fattispecie penali previste nel nostro ordinamento tutelano in via secondaria e derivata una pluralità di interessi, magari nemmeno tutti considerabili veri e propri "beni giuridici". Inoltre la categoria della plurioffensività è duramente criticata da varie voci in dottrina[22], poiché rende le fattispecie penali di difficile inquadramento ed è da molti Autori percepita come un facile espediente per non identificare quale sia il reale bene giuridico che, nella specifica norma, il legislatore intende tutelare. Fiandaca sostiene che il bene giuridico, oltre ad essere "*canone legislativo di criminalizzazione*", assolve altresì una funzione "*dogmatica*", facendo in modo che l'individuazione degli elementi tipici della fattispecie includa l'effettiva lesione del bene giuridico. Presupporre che una fattispecie possa essere lesiva di una pluralità di beni giuridici comporta il rischio di un equivoco ermeneutico nel momento in cui si riscontra la lesione di alcuni e non di altri: l'interprete è portato a chiedersi come si pongono i beni in rapporto fra loro, o se si debba creare una sorta di gerarchia interna ad ogni singola disposizione incriminatrice per capire quando la violazione ha rilevanza penale. Sono domande pericolose, poiché possono condurre l'operatore del diritto a considerare inapplicabile una determinata fattispecie quando in realtà il bene giuridico da essa tutelato è pienamente offeso.

La frode informatica è inclusa dalla maggior parte degli Autori fra i reati mono-offensivi; cionondimeno possono essere individuati altri beni giuridici che vengono tutelati in via secondaria dalla stessa. Si tratta di una fattispecie posta a tutela del patrimonio che però irradia la propria tutela anche nei confronti della sicurezza delle comunicazioni e transazioni informatiche, della riservatezza che deve accompagnare l'utilizzo dei sistemi informatici e telematici e del loro

[21] F. Antolisei, "*Manuale di diritto penale, Parte speciale, I*", Giuffré, Milano, 2002, pag. 374

[22] G. Fornasari si esprime in termini critici verso la categoria della plurioffensività in molti suoi scritti, fra i quali vedi A. Bondi, A. Di Martino, G. Fornasari, "*Reati contro la pubblica amministrazione*", Giappichelli, 2008. Inoltre, Fiandaca, E. Musco, *"Diritto penale, Parte Generale*", Zanichelli Ed., VI ed., 2009.

regolare funzionamento[23].

Anche in giurisprudenza si registrano posizioni differenti: parte maggioritaria ha sostenuto fin dalle prime applicazioni che l'art. 640-ter c.p. è stato introdotto a presidio del patrimonio, per rimediare ai vuoti di tutela derivanti dall'inapplicabilità del reato di truffa[24]. Nondimeno, un orientamento minoritario (avallato anche dalla Corte di Cassazione) è propenso a configurare tale fattispecie come reato plurioffensivo, posto a presidio "*della riservatezza e della regolarità dei sistemi informatici [nonché] del patrimonio altrui*"[25].

Con riguardo al bene giuridico tutelato dalla nuova aggravante inserita al comma 3 dell'art. 640-ter c.p., sono prospettabili due ricostruzioni.

Muovendo da dati formali, quali i lavori preparatori al d.lgs. n. 93 del 2013, la struttura e la collocazione della nuova ipotesi di frode informatica con "*furto o indebito utilizzo di identità digitale*" e il riferimento ad essa come "aggravante" nello stesso art. 640-ter c.p., si arriva a configurare la condotta come un'ipotesi aggravata di frode informatica, come tale posta a presidio del medesimo bene giuridico, il patrimonio[26]. Quindi possono valere le medesime considerazioni svolte con riferimento alla fattispecie base.

La seconda impostazione, invece, più sostanzialistica, individua come tratto caratterizzante della nuova condotta proprio il "furto o indebito utilizzo di identità digitale": in questo modo il c. 3 art. 640-ter c.p. si configurerebbe come un'autonoma fattispecie delittuosa, posta a presidio della libertà informatica, intesa come libertà di utilizzare i propri dati personali in ambiente informatico e della sicurezza delle transazioni virtuali. Ancor più in questo caso potrebbe

[23] Nel senso che la fattispecie di frode informatica è posta a presidio di interessi ulteriori al patrimonio, quali la riservatezza in ambito informatico e il regolare funzionamento del sistema, G. Fiandaca – E. Musco, "*Diritto penale, Parte speciale, I delitti contro il patrimonio*", Bologna, 2002; A. Pagliaro, "*Principi di diritto penale, Parte speciale, Delitti contro il patrimonio*", Milano, 2003; F. Antolisei, "*Manuale di diritto penale, Parte speciale, I*", Milano, 2002.

[24] Cass. Pen. Sez. VI, n. 3065 del 14/12/1999 (ud. del 04/10/1999), *De Vecchis*; Cass. Pen. Sez. VI, n. 3067 del 14/12/1999 (ud. del 04/10/1999), *Piersanti*; Cass. Pen. Sez. V, n. 1727 del 30/09/2008 (ud. del 30/09/2008).

[25] In tal senso, Cass. Pen., sez. V, sent. n. 4576 del 24/11/2003.

[26] Dossier del Servizio studi sull' A.S. n. 1079 "*Conversione in legge, con modificazioni, del decreto-legge 14 agosto 2013, n. 93, la "furto o indebito utilizzo di identità digitale" in luogo della locuzione "sostituzione di identità digitale", impiegata dal decreto-legge*", edizione provvisoria, ottobre 2013, n. 64, pag. 103, in www.senato.it; A. Di Tullio D'Elisiis, "*Frode informatica commessa con sostituzione d'identità digitale: profili applicativi*", articolo del 14/01/2014, reperibile su Altalex, http://www.altalex.com/index.php?idnot=66034#_ftn3

prospettarsi una ricostruzione come fattispecie plurioffensiva, in cui all'offesa al patrimonio si affianca quella alla riservatezza come diritto della personalità. Per evitare l'utilizzo della categoria della plurioffensività, è possibile prospettare una nuova ricostruzione del concetto di patrimonio, nella quale includere anche i dati inerenti il singolo diffondibili nella rete.

Qualche considerazione infine appare opportuna relativamente all'oggetto di tutela della fattispecie di indebito utilizzo di carte di debito o di pagamento di cui all'art. 55 c. IX d.lgs. n. 231/2007[27].
La disposizione è stata introdotta nell'ambito di un intervento legislativo di più ampio respiro, finalizzato da un lato a contrastare il fenomeno del riciclaggio di denaro di provenienza illecita attraverso una politica tesa a limitare l'utilizzo del denaro contante e dei titoli al portatore; dall'altro a rafforzare la fiducia dei consumatori nell'utilizzazione dei circuiti elettronici di pagamento.
La risposta penale è sembrata la migliore dal punto di vista della prevenzione generale e della deterrenza.
In tale ipotesi la natura della fattispecie è "ontologicamente" duplice e rende molto complessa l'individuazione di un unico bene giuridico oggetto di tutela: con la sua introduzione infatti il legislatore ha guardato non solo al possibile *vulnus* all'interesse pubblico derivante da transazioni in cui viene riciclato denaro "sporco", ma anche alla possibile lesione patrimoniale sofferta dal singolo titolare di carta di debito o di credito derivante da transazioni illegittimamente portate a termine.
Si tratta di una problematica di notevole rilevanza poiché, dalla risoluzione in un senso piuttosto che in un altro, derivano importanti conseguenze, quali ad esempio la possibilità di concorso con i reati di truffa ovvero di frode informatica.

[27] La disposizione in commento stabilisce: "*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, è punito con la reclusione da uno a cinque anni e con la multa da 310 a 1.550 euro. Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per altri, falsifica o altera carte di credito o di pagamento o qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, ovvero possiede, cede o acquisisce tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi*".

Nei primi anni di applicazione della fattispecie, la tendenza fu quella di dare rilevanza soprattutto alla prospettiva pubblicistica dell'oggetto giuridico. Si considerava bene meritevole di tutela penalistica "*il diritto incorporato nel documento*", ossia la facoltà di fruire di determinati beni attraverso l'utilizzazione del documento stesso. La tutela penale non doveva investire la carta di debito o credito in quanto tale, ma operava come catalizzatore per stimolare la circolazione di beni[28]. Presto però la "natura composita" del bene giuridico è stata rilevata in alcune sentenze della Corte di Cassazione[29], nelle quali il giudice di legittimità ha inserito fra i beni tutelati dalla norma in commento non solo un possibile *vulnus* alla pubblica fede (concetto che rimane fortemente discusso in dottrina), ma altresì la lesione di tipo privatistico agli interessi patrimoniali del titolare della carta.

Il panorama dottrinale e giurisprudenziale è mutato dopo un intervento di "*overruling*" della Cassazione a Sezioni Unite nel 2001, confermato poi anche nel 2005[30], e ad oggi sembra essersi assestato sulla concezione privatistica del bene oggetto di tutela: si ritiene che l'art. 55 c. IX sia stato inserito nell'ordinamento a tutela in primis del patrimonio del singolo titolare di carta di pagamento, posto in pericolo dall'utilizzazione indebita da parte di terzi di tali documenti elettronici[31]. Non deve confondersi la *ratio* dell'intervento legislativo

---

[28] "*La ratio della norma è proprio la tutela dell'incorporazione in un documento di beni "ulteriori" rispetto al valore del medesimo, per facilitarne la circolazione, siano essi denaro* (come nel caso del prelievo del contante), *altri beni* (di qualsiasi natura, quindi anche generi alimentari, ovvero benzina) *e soprattutto servizi*", così in Cass. Pen., sez. I, sent. n. 37115 del 5/11/2002.

[29] Cass. Pen., sez. V, sent. n. 23429 del 8/06/2001.

[30] Cass. Pen., sez. V, sent. n. 6695 del 12/12/2005 e Cass. Pen., sez. Unite penali, 28/03/2001, *Tiezzi.* In tale sede, la Suprema Corte tratta in maniera analitica la problematica del concorso fra la fattispecie in discorso (nella versione del 1991) e il delitto di truffa: la Corte, capovolgendo l'orientamento prevalente anche fra le Sezioni Penali, stabilisce che si è di fronte ad un caso di specialità reciproca (per una riflessione in proposito vedi *infra*) e argomenta la sua posizione anche riferendosi all'oggetto giuridico. "*L'offesa al patrimonio individuale non è affatto estranea alla ratio incriminatrice dell'art. 12, come è stato più volte affermato ed è stato ribadito dalla Corte costituzionale con la sentenza n. 302 del 19/7/2000, la quale ha basato il giudizio di infondatezza della questione di legittimità costituzionale dell'art. 649 c.p., nella parte in cui non comprende tra i fatti non punibili, se commessi in danno dei congiunti ivi indicati, quelli previsti dall'art. 12 del D.L. n. 143/91, sul carattere concorrente con l'offesa al patrimonio individuale dell'aggressione di valori riconducibili all'ambito dell'ordine pubblico o economico e della fede pubblica".* Le due norme tutelano da prospettive diverse sempre il patrimonio, essendo l'indebito utilizzo di carte di pagamento una possibile manifestazione degli "artifizi e raggiri" ex art. 640 c.p. Vedi par. *infra* cap. IV par. 1.

[31] C. Pecorella, "*Diritto penale dell'informatica*", Cedam, Padova, 2006; R. Borruso, "*Gli aspetti legali nella sicurezza nell'uso delle carte di credito e di pagamento*", in Giust. Civ., 1992.

con il bene giuridico tutelato: la fede pubblica e l'interesse pubblico alla regolarità e alla trasparenza della transazioni sono tutelate solo in via mediata ed indiretta.

2.2 Ratio dell'innovazione normativa: il (difficile) rapporto con la fattispecie tradizionale di truffa. L'elemento implicito.

La frode informatica ha trovato la sua ragion d'essere nell'ordinamento proprio in rapporto alla truffa: non vi è dubbio che il legislatore del 1993 scelse di introdurre tale fattispecie per rimediare alle difficoltà applicative dell'art. 640 c.p. nell'ambiente informatico.

Il problema principale era rappresentato dall'individuazione del requisito tipico dell'"*induzione in errore*": si riteneva che tale elemento, caratteristico della truffa, fosse di fatto assente nel caso di condotte poste in essere da un agente direttamente su un elaboratore di dati (sprovvisto delle facoltà cognitive proprie dell'essere umano). L'induzione in errore presuppone di necessità una relazione interpersonale connessa ad un'attività fraudolenta svolta da uno dei due soggetti[32]: la vittima coopera artificiosamente con l'agente, consentendo ad un negozio giuridico avente natura patrimoniale, sulla base di una falsa rappresentazione della realtà causata dagli artifici e raggiri.

Nel caso di frode mediante Personal Computer, si ha un rapporto mutuamente esclusivo fra uomo ed elaboratore di dati: la vittima quindi non avrebbe potuto avvalersi della tutela ex art. 640 c.p., non essendo portata ad "auto-danneggiarsi". Spesso, infatti, il soggetto vittima delle condotte fraudolente in ambito informatico è del tutto estraneo all'attività indebita dell'operatore e diventa "parte" dell'operazione solo dopo aver scoperto il danno patrimoniale subito. Anche volendo applicare la fattispecie di truffa alle ipotesi informatiche, sarebbe stato oltremodo complesso, da un lato, superare la dottrina tradizionale che richiede l'atto di disposizione patrimoniale da parte del soggetto passivo della truffa; dall'altro, dimostrare la rappresentazione e volontà di indurre taluno

[32] In tal senso, L. Picotti, *"Il diritto penale dell'informatica nell'epoca di Internet"*, Cedam, Padova, 2004.

in errore in un soggetto che si limita ad immettere dei comandi in un elaboratore. Con la conseguenza che il requisito del dolo sarebbe rimasto talmente controverso da condurre spesso all'impunità con la formula "*il fatto non costituisce reato*".

E' bene sottolineare che si trattava di dubbi attinenti al piano prettamente formale e giuridico-teorico: nessuno dubitava che nei fatti si fosse di fronte sostanzialmente ad una condotta meritevole di sanzione, per molti versi assimilabile ad una truffa[33].

Vi erano Autori che già avevano saputo intravedere l'equivoco in cui il panorama dottrinale stava incorrendo, forse sull'onda dell'entusiasmo dovuto alla novità del fenomeno informatico: costoro rilevavano come il PC fosse meramente uno strumento (in quanto *software*) attraverso il quale si estrinseca la volontà dell'agente, quindi "*interagire maliziosamente con esso profittando dei suoi punti deboli è come trarre in inganno l'uomo stesso che lo usa*"[34]. Si è parlato di "sofisma ad effetto": sarebbe stato sufficiente interpretare la fattispecie tradizionale "come se" l'induzione in errore avvenisse nei confronti di una persona fisica[35]. Si trattava di un opinione molto interessante ed innovativa per gli anni Novanta del secolo scorso; oggi sarebbe forse più facilmente sostenibile data la pervasività ed il massiccio utilizzo di strumenti tecnologici in qualsivoglia settore d'attività. Tuttavia si poteva facilmente replicare che in questo modo si rischiava un *vulnus* del principio di determinatezza che poteva condurre ad ipotesi di analogia *in malam partem*, assolutamente vietate anche a livello costituzionale (art. 25 Cost.)[36].

---

[33] G. Pica, *op. cit.*

[34] R. Borruso, G. Buonuomo, G. Corasaniti, D'Aietti, "*Profili penali dell'informatica"*, Giuffré, Milano, 1994, pag. 34

[35] R. Borruso, G. Buonuomo, G. Corasaniti, D'Aietti, *op. cit.*

[36] Bisogna rilevare che non tutti gli Stati scelsero di introdurre una fattispecie ad hoc per le frodi informatiche. In Francia, ad esempio, tale necessità non è stata avvertita: è stata ritenuta sempre applicabile la disposizione tradizionale in materia di truffa, alla luce dell'interpretazione giurisprudenziale estensiva dei suoi elementi costitutivi (requisito dell'induzione in errore, oggi esplicitato, può riferirsi indifferentemente ad una persona fisica o ad una persona giuridica; la nozione di *manoeuvres frauduleuses* è molto ampia e include anche comportamenti diretti all'uomo solo in via mediata). Non si è intervenuti nemmeno con l'introduzione del codice penale del 1994: in esso trovano collocazione altre fattispecie informatiche, come l'accesso abusivo. Anche la disposizione sulla truffa contenuta nel c.p. canadese è stata ritenuta applicabile in ambito informatico, dato che la condotta fraudolenta può realizzarsi sia "by

Dal canto suo, la giurisprudenza prevalente non riusciva a superare "l'ostacolo informatico", forse per mancanza di conoscenze tecniche al riguardo, forse per il timore di aspre critiche se si fosse addentrata su un cammino interpretativo troppo innovatore: le imputazioni ante 1993 vedevano l'utilizzo di fattispecie come la truffa in concorso con il falso, in alcuni casi di manomissione di dati a fini di indebito profitto, oppure in altri casi si è scelto di non contestare autonomamente il delitto di falso, eludendo così il problema relativo al fatto se potessero essere considerati "documenti" a fini penalistici i dati immessi in un elaboratore. In tal modo era possibile, per lo meno nei casi in cui vi erano persone fisiche preposte al controllo dei sistemi informatici, superare il problema applicativo della truffa riferendo l'induzione in errore di "taluno" a codesti soggetti che dovevano verificare il corretto funzionamento dell'elaboratore elettronico[37].

Ad ogni modo, si riteneva comunemente che non potesse sussistere una reale equiparazione fra induzione in errore di una persona fisica e induzione in errore di un programma per elaboratore, praticamente impossibile.

Senza dubbio quindi l'introduzione dell'art. 640-ter c.p. ha avuto il merito di portare più certezza nel panorama legislativo italiano: le scelte effettuate relativamente alla struttura della fattispecie però si distanziano da quelle di altri Stati, dove la somiglianza con la struttura del delitto di truffa è più marcata[38], legittimando l'idea che in Italia si sia voluto optare per una fattispecie autonoma. Ciononostante, a parere di un certo orientamento dottrinale[39] che si basa su identità dell'oggetto giuridico e ratio della fattispecie – e che trova ancora grande consenso in ambito giurisprudenziale – il delitto di frode informatica

---

deception" sia attraverso "other fraudulent means": non è necessaria la prova di una relazione fra autore e vittima. C. Pecorella, *op. cit*.

[37] Rispettivamente, G. Pica, *op.cit*., pag. 160-161: caso giudicato dal Trib. Como, sez. pen., 1995, n. 611. C. Sarzana di S. Ippolito, "*Informatica, internet e diritto penale*", Giuffré, 2010, pag. 237-239: sentenza del Trib. Roma, 1983, imp. *Testa ed altri*, confermata in appello nel 1985, in *Diritto dell'informazione e dell'informatica*, 1986. Si trattava per lo più di casi in cui, mediante l'introduzione di dati falsi nel sistema, si facevano figurare contributi INPS non versati. Il soggetto direttamente indotto in errore era l'operatore INPS.

[38] Molti Stati, fra cui Germania, Austria, Svezia, Grecia, utilizzarono il medesimo schema causale alla base del delitto di truffa: condotta fraudolenta, che si sostanzia nella manipolazione del procedimento di elaborazione dati, la quale è causa di una alterazione del risultato di tale procedimento, la quale è causa a sua volta di un danno al patrimonio altrui. Classica configurazione di reato d'evento, in cui la condotta è pressoché libera. C. Pecorella, *op. cit.*

[39] G. Pica, *op. cit.*

costituisce un'ipotesi speciale rispetto a quella generale di truffa.

La fattispecie di truffa non riusciva ad apprestare una tutela effettiva in tutti quei casi di condotte fraudolente aventi ad oggetto o realizzate mediante sistemi informatici o telematici che comportassero un indebito arricchimento con danno altrui. Spesso infatti, le condotte poste in essere in ambito informatico non hanno un destinatario persona-fisica ben determinato: l'agente si limita ad introdurre nel sistema comandi o programmi che gli permettano di profittare indebitamente delle risorse di altri contenute nell'ambiente virtuale.

Secondo tale orientamento, l'intervento legislativo era in primis volto a portare più certezza relativamente alla illiceità penale di tali condotte: tuttavia la vera e sola novità era la tipizzazione degli artifizi e raggiri e la mancanza dell'induzione in errore. Per il resto, ci si trovava di fronte ad una truffa.

A sostegno di tale orientamento, alcuni sottolineavano anche la scelta nella rubrica dell'art. 640-ter c.p. (seppur si tratta di un elemento non vincolante): il legislatore, conscio dell'assenza in questi casi dell'induzione in errore, aveva preferito introdurre la fattispecie con il termine più generale e omnicomprensivo di frode, anziché parlare di truffa[40].

L'elemento degli "artifizi e raggiri con induzione in errore" è stato sostituito con la tipizzazione delle condotte fraudolente: l'art. 640-ter c.p. richiede l'intervento fraudolento su un elaboratore commesso mediante "*alterazione […] del funzionamento di un sistema informatico o telematico*" o "*intervento […] su dati, informazioni o programmi contenuti in un sistema informatico o telematico*".

Da tali premesse questi Autori sostenevano che la frode informatica costituisse semplicemente una fattispecie speciale ricompresa nel *genus* della truffa, senza autonomia applicativa: si trattava di una fattispecie suppletiva, creata per sanzionare quelle condotte che non si riusciva a punire attraverso la truffa tradizionale.

G. Pica arrivò a sostenere che i due reati si distinguono unicamente per "*le concrete modalità di commissione*", richiamandosi alla Relazione governativa: peraltro si sarebbe anche potuto procedere con la semplice modifica dell'art.

[40] A. Manna, "*Artifici e raggiri on-line: la truffa contrattuale, il falso informatico e l'abuso dei mezzi di pagamento elettronici*", in Diritto dell'informazione e dell'informatica, 2002, 995

640 c.p., introducendo "*un ulteriore comma relativo ai casi di truffe commesse con tecnologie informatiche*"[41].

Negli anni successivi, vari Autori hanno iniziato a distaccarsi da tale orientamento, sostenendo che certamente la frode informatica si ispira allo schema della truffa, della quale infatti dovrebbe costituire una figura affine[42]; ciononostante presenta caratteristiche assolutamente nuove e peculiari che la allontanano dal modello di partenza e permettono di individuare per essa una sostanziale dimensione d'autonomia concettuale e applicativa[43].

A riprova di ciò, il legislatore italiano, a differenza di alcuni legislatori stranieri[44], ha scelto di non richiedere espressamente per la frode informatica la stessa concatenazione causale che caratterizza la truffa: in particolare, non ha introdotto nella fattispecie l'elemento del risultato irregolare del processo di elaborazione di dati conseguente alla condotta fraudolenta dell'agente, da cui deriverebbe causalmente il danno al patrimonio con indebito arricchimento[45].

Il focus della disposizione italiana è tutto sulle condotte, non sul risultato non conforme alle aspettative del legittimo operatore del sistema: in tal modo si è inteso evitare che il concreto *modus operandi* dell'agente diventasse irrilevante e si è delimitato più precisamente il confine applicativo della fattispecie, includendo anche quei casi in cui non è pienamente dimostrabile l'interferenza con il risultato del processo di elaborazione preventivato dall'operatore.

È vero che le due condotte previste all'art. 640-ter c.p. vengono poi ampliate, poiché possono realizzarsi "*in qualsiasi modo*" ovvero "*con qualsiasi modalità*": ma è altrettanto vero che la condotta deve necessariamente ed inderogabilmente consistere in una delle due tipizzate dalla norma.

In base a tale ricostruzione, parte della dottrina e della giurisprudenza ritengono che l'ingiusto profitto con altrui danno derivi direttamente dalla condotta dell'agente[46]: il giudice deve solamente verificare che vi sia stata un'alterazione

---

[41] G. Pica, *op.cit.,* pag. 141
[42] Camera dei Deputati, IX Legislatura, Disegno di Legge n. 2773
[43] C. Pecorella, *op.cit.*
[44] Si segnalano il codice penale spagnolo, il codice penale tedesco, il codice penale austriaco e il codice penale portoghese. C. Pecorella, *op.cit.*
[45] C. Pecorella, *op.cit.* pag. 63 e segg.
[46] S. Logroscino, "*La frode informatica quale autonoma figura di reato rispetto al delitto di truffa*", 21/12/2011, Altalex: http://www.altalex.com/index.php?idnot=16607

del funzionamento o un intervento senza diritto sul sistema informatico o telematico, da cui sia derivato causalmente e direttamente il profitto dell'agente o di terzi con altrui danno. Non deve preoccuparsi di verificare se la condotta dell'agente abbia causato una manomissione del sistema[47], che ha così eseguito operazioni irregolari, o se il sistema in sé considerato funzioni regolarmente e siano semplicemente stati aggiunti o eliminati dei dati: non si è voluto, in altri termini, onerare l'operatore giuridico di un compito molto complesso, che può richiedere la conoscenza tecnica specifica dei singoli sistemi informatici e di trattamento dati[48].

La disposizione italiana appare sicuramente originale: non essendo richiesto espressamente un elemento che nella truffa è fondamentale e che molti legislatori richiedono (l'induzione in errore della vittima, trasposto in ambito informatico dalle disposizioni di altri ordinamenti come "causazione di un risultato inesatto o irregolare nel processo di elaborazione dati"), emerge la volontà del legislatore interno di definire in maniera indipendente la struttura ed i confini della fattispecie di cui all'art. 640-ter c.p., separandola in maniera netta dall'alveo applicativo della truffa, per farle assumere il ruolo di ipotesi delittuosa autonoma, non meramente suppletiva rispetto alla truffa tradizionale, volta a sanzionare quei casi in cui nella causazione del profitto e del danno non è coinvolto in prima persona il soggetto frodato: l'azione colpisce in via diretta l'elaboratore ma l'offesa al bene giuridico ricade poi in via indiretta su una persona (fisica o giuridica). Si tratta quindi di uno strumento fondamentale per sanzionare anche condotte strutturalmente differenti dalle truffe del mondo reale.

Proprio a questo punto però emergono le criticità ed i rischi in cui può incorrere un'impostazione fin troppo aderente alla *littera legis* e che non tiene conto a sufficienza dell'esperienza criminologica, la quale ha mostrato come sia una

[47] Peraltro in tal caso potrebbe sussistere anche un danneggiamento informatico, autonomamente sanzionabile ex art. 635-bis c.p.

[48] Emerge ancor più evidente la differenza con la truffa, in cui gli "artifici e raggiri" possono risultare di equivoca interpretazione (data anche la necessità che siano in grado in concreto di "sorprendere l'altrui buona fede"); nel caso di frode informatica, l'analisi si concentra sugli interventi e sulle alterazioni di sistema, che possiedono un coefficiente di espressività criminale più elevato e sono di più semplice accertamento. M. Romani, D. Liakopoulos, "*La globalizzazione telematica*", Giuffré, 2009, pag. 232

costante dei casi di frode informatica la lesione della sfera patrimoniale altrui attraverso l'interferenza con l'esito regolare del processo di elaborazione[49].

La dichiarata assenza di un evento intermedio (che peraltro viene sempre rivenuto nell'esperienza criminologica) rischia di far ricondurre alla frode informatica pure quei casi nei quali la lesione al patrimonio altrui si realizza indipendentemente dall'esito del processo di elaborazione manipolato. L'interprete può essere tentato di applicare l'art. 640-ter c.p. allorquando è la stessa azione fraudolenta ad incidere direttamente sugli interessi economici altrui ovvero alle ipotesi nelle quali l'esito manipolato del processo di elaborazione è solo un passaggio prodromico per una successiva condotta di aggressione: ma si tratta di casi in cui la dinamica dell'offesa è affatto diversa da quella consueta delle frodi, informatiche e non, e che trovano presidio in ambito penale grazie ad altre fattispecie, nell'un caso quella di danneggiamento informatico (essendo palese che se il danno al patrimonio deriva direttamente dalla condotta dell'agente, non vi è stato nessuno spostamento patrimoniale) nell'altro con la fattispecie di furto aggravato dall'impiego di mezzi fraudolenti[50].

Le fattispecie di frode sono poste senza dubbio a presidio del patrimonio ma la condotta fraudolenta non si sostanzia in una aggressione diretta e immediata allo stesso: l'inclusione nell'art. 640-ter delle ipotesi sopra menzionate risulterebbe non solo superflua, trattandosi di fatti già penalmente rilevanti ad altro titolo, ma del tutto anomala nell'ambito dei delitti contro il patrimonio.

Alla frode informatica devono quindi rimanere estranei tutti quei casi in cui il collegamento causale fra l'alterazione del risultato del processo e il profitto ingiusto con altrui danno è totalmente assente o soltanto indiretto.

Il profitto ingiusto e il danno altrui devono avere una fonte immediata e diretta che funga da anello di congiunzione con le condotte fraudolente. Negli altri ordinamenti essa viene per lo più prevista espressamente ex lege; nel nostro sistema, tale requisito deve essere integrato in via interpretativa e si tratta dello stesso rinvenuto nella fattispecie di truffa come "atto di disposizione

[49] C. Pecorella, *op.cit*., pag. 112

[50] Non sono mancati autorevoli Autori che hanno sottolineato proprio la vicinanza della frode informatica con tale categoria di illeciti, F. Mantovani, *"Diritto penale, parte speciale – Delitti contro il patrimonio*", Cedam, Padova, 2002, pag. 209.

patrimoniale", ma declinato in ambito informatico come "risultato irregolare di un processo di elaborazione"[51].

Vi sono stati anche Autori i quali, volendo rimanere più aderenti al dato letterale, hanno proposto una diversa interpretazione della fattispecie, sostenendo che tale evento intermedio, sebbene non menzionato espressamente dall'art. 640-ter c.p., andrebbe comunque sempre rinvenuto in tutte le ipotesi di "alterazione del funzionamento del sistema", poiché il concetto stesso di alterazione presuppone che vi sia stato un cambiamento con altro[52] rispetto allo stato iniziale: perciò, essendo ontologicamente connaturato ad ogni alterazione un risultato irregolare nel funzionamento, non è necessario che esso sia previsto in via espressa dalla disposizione. Questa posizione è stata spesso condivisa anche dalla giurisprudenza di legittimità, quando individua l'alterazione del funzionamento in "*ogni attività o omissione che, attraverso la manipolazione dei dati informatici, incida sul regolare svolgimento del processo di elaborazione e/o trasmissione dei suddetti dati e, quindi, sia sull'hardware che sul software*"[53].

La regolarità dell'esito del processo va commisurata in concreto, sulla base dei risultati che il proprietario o legittimo utilizzatore del sistema aveva preventivato sarebbero derivati dai comandi *input* pre-immessi: non si tratta quindi di regolarità o irregolarità misurate sulla base di un canone di offensività in astratto, potendo configurarsi un risultato irregolare anche senza un danno effettivo ai sistemi[54].

Si comprende come la preoccupazione di una *overcriminalization* delle aggressioni informatiche è stata affrontata in modi differenti dai legislatori che si sono occupati di tale problema: da un lato, molti di loro hanno preferito formulare disposizioni che, pur essendo rivolte a sanzionare condotte informatiche, non oltrepassassero i confini applicativi della fattispecie di truffa,

[51] Anche Mucciarelli ritiene che la fattispecie di frode informatica presenti un requisito costitutivo inespresso, rappresentato dalla disposizione patrimoniale posta in essere dal sistema informatico o telematico, a ciò abilitato, F. Mucciarelli, "*Commento all'art. 10 della l. 23/12/1993 n. 547"*, in Legislazione Penale, 1996, pag. 138

[52] Alterazione dal latino *alteratio*, da *alter* che significa "altro (fra due)".

[53] Cass. Pen*.,* sez. II, sent. n. 13475 del 06/03/2013*.*

[54] Per esemplificare, una condotta manipolativa che comporta lo spostamento patrimoniale illegittimo di una somma di denaro da un conto corrente ad un altro non configura un risultato che danneggia i sistemi; viene semplicemente immesso nel sistema un comando indebito che comporta un risultato non conforme alle aspettative del legittimo utilizzatore.

richiedendo così la medesima sequenza causale solamente trasposta in ambiente virtuale. In questo modo i confini applicativi della fattispecie tradizionale avrebbero guidato e limitato l'applicazione delle norme di nuovo conio.

Dal canto suo, il legislatore italiano ha optato per una individuazione dei confini applicativi della norma attraverso una più tecnica tipizzazione delle condotte penalmente rilevanti ma evitando di richiedere espressamente la causazione di un risultato inesatto: si è così evitato di concentrare l'attenzione dell'interprete su un evento virtuale complesso da dimostrare in maniera specifica. L'ampiezza della fattispecie deriva direttamente dalla elaborazione dottrinale e giurisprudenziale formatasi sulle condotte stesse.

Ciò posto, è indiscutibile che truffa e frode informatica abbiano elementi in comune, in primo luogo gli elementi dell'ingiusto profitto e dell'altrui danno[55]; per essi è sicuramente possibile – e doveroso – utilizzare l'elaborazione teorica e pratica sviluppatasi con riguardo alla fattispecie tradizionale, art. 640 c.p.

Anche la giurisprudenza, di merito come di legittimità, appare oscillante: si registrano decisioni propense a considerare la frode informatica una *species* di truffa[56], pur evidenziando che vi sono dei tratti peculiari della stessa, e altre in cui si afferma chiaramente come "*la fattispecie di cui all'art. 640-ter integri senz'altro un'autonoma figura di reato, a differenza di quanto si è invece ritenuto a proposito della ipotesi di truffa aggravata per il conseguimento di erogazioni pubbliche*"[57].

La stessa Corte di Cassazione ha rilevato che "*la novella tracciata ex art. 640-ter c.p. […] ha la medesima struttura e quindi i medesimi elementi costitutivi della truffa, dalla quale si differenzia solamente perché l'attività fraudolenta dell'agente investe non la persona (soggetto passivo), di cui difetta l'induzione in errore, bensì il 'sistema informatico' di pertinenza della medesima, attraverso*

[55] Su questo punto vedi *infra* cap. II par. 6-7.

[56] Ad esempio, Cass. Pen., sez. VI, sent. n. 8755 del 26/02/2009 in cui si afferma *expressis verbis* che "*il reato di frode informatica altro non è che una ipotesi specifica di quella di truffa*"; in Cass. Pen., sez. II, sent. n. 18909 del 30/04/2013 si parla espressamente di "*truffa informatica*".

[57] Cass. Pen., sez. II, sent. n. 17748 del 15/04/2011.

la manipolazione di detto sistema"[58]. Questo è un punto ribadito più volte dai giudici di legittimità, tuttavia senza chiarire fino in fondo la natura della fattispecie.

L'unica peculiarità individuata con certezza è costituita proprio dal soggetto passivo della condotta e dal fatto che, per quanto concerne gli altri elementi, il riferimento corre all'elaborazione giurisprudenziale tradizionale[59].

2.3 Le condotte tipiche: previsioni autonome o condotta unica?

Si è già avuto modo di approfondire la scelta del legislatore italiano di individuare la fattispecie di frode informatica puntando l'attenzione sulle modalità delle condotte con cui si interviene abusivamente, piuttosto che sulle conseguenze da esse provocate sul processo di elaborazione dati. Ora l'analisi si concentrerà sulle singole condotte tipiche, cercando di definire in concreto l'ambito applicativo.

Preliminarmente però è necessario un riferimento agli orientamenti dottrinali e giurisprudenziali sviluppatisi sulla natura delle due condotte.

La prima concezione, facendo leva sull'identità della frode informatica con il reato di truffa, individuava un'unica condotta tipica nel delitto di cui all'art. 640-ter c.p., consistente nel "*procurare a sé o ad altri un ingiusto profitto con altrui danno*": si rinveniva solo una differenza nelle concrete modalità di realizzazione del profitto, nella frode informatica dettagliatamente previste, nella truffa descritte in modo sintetico e omnicomprensivo[60].

"*Alterazione del sistema"* e "*intervento senza diritto*" sarebbero la specificazione in ambito informatico degli artifizi e raggiri propri della truffa, in quanto attraverso di essi viene modificata la logica di funzionamento regolare della macchina, per farle compiere operazioni di trattamento ed elaborazione dati che conducono a risultati non voluti dal titolare e indebitamente vantaggiosi per l'agente. Essendo mere concretizzazioni di un concetto più generale ed

[58] Cass. Pen. sent. n. 8755 del 26/02/2009,; nello stesso senso Cass. Pen. sent. n. 4576 del 05/02/2004,; Cass. Pen., sez. VI, sent. n. 3065 del 4/10/1999, *De Vecchis*.
[59] Da ultimo ribadito in Cass. Pen. sez. II, sent. n. 18909 del 10/04/2013.
[60] G. Pica, *op.cit.*

omnicomprensivo, inoltre, non possono configurarsi come autonome ed alternative: pur essendo legate dalla disgiuntiva "o", non si tratterebbe di condotte concettualmente del tutto separate. La seconda ipotesi ("intervento senza diritto su dati, informazioni o programmi") implica infatti necessariamente che il sistema informatico o telematico venga in qualche modo alterato nelle sue componenti hardware o software precedentemente programmate; quindi l'unica vera modalità di commissione prevista sarebbe "l'alterazione di sistema". Ad avvalorare tale opinione si rileva come, nella maggior marte dei casi, l'ulteriore condotta di intervento venga assorbita dalla prima e costituisca un'azione preparatoria ed induttiva dell'alterazione del funzionamento: il legislatore perciò ha voluto inserirla nella fattispecie esclusivamente al fine di rimuovere ogni possibile dubbio sulla rilevanza penale della condotta[61].

Da tale ragionamento si fa discendere l'ulteriore conseguenza della maggior determinatezza delle condotte meritevoli di sanzione penale[62].

Fra coloro che invece cercarono e ancor oggi cercano di individuare con precisione una dimensione applicativa autonoma per le due condotte, le posizioni sono eterogenee: vi sono stati Autori che hanno ricondotto la distinzione al tipo di modificazione posta in essere, estrinseca e strutturale nel caso di alterazione del sistema, intrinseca e condizionante le singole istruzioni impartite nel caso di intervento senza diritto[63]. Altri Autori hanno sostenuto che la differenza sta nell'ampiezza dell'intervento, più incisivo nel caso della prima condotta, poiché colpisce l'intero sistema informatico o telematico; isolato sul singolo dato informatico, la singola informazione o il singolo programma nel secondo caso[64]. Altri ancora hanno sostenuto che la fattispecie si compone di due condotte, di cui la seconda opera solo in via residuale, quando cioè si vuole

[61] G. Pica, *op.cit*., pag. 144

[62] Sul punto comunque le posizioni non sono univoche: vedi *infra* nota 69.

[63] C. Parodi, "*La frode informatica: presente e futuro delle applicazioni criminali nell'uso del software*, in Diritto penale processuale, 1997, pag. 1538. Nel primo caso si pensi ad una condotta di danneggiamento informatico o all'inserimento di virus, al fine di paralizzare in via temporanea o modificare indebitamente le funzionalità di un programma operativo; nel secondo caso, invece, il riferimento corre ai casi di inserimento surrettizio in un sistema di dati di individui, al fine di poter usufruire di prestazioni previdenziali (*data-diddling*), oppure alle modificazioni di programma attraverso l'inserimento di un codice che consente di fruire di profitti indebiti a danno di un numero imprecisato di utenti (*salami tecnique*).

[64] D. D'Agostini, "*Diritto penale dell'informatica – Dai computer crimes alla digital forensic*", Esperta, Forlì, 2007, pag. 62

dare rilevanza penale ad una forma di interferenza diversa da una vera e propria alterazione di sistema, la quale pur tuttavia sia caratterizzata da una propria carica offensiva[65].

In realtà, per capire il rapporto fra le due condotte tipiche, è necessario partire da un dato fondamentale: l'unicità del reato previsto all'art. 640-ter c.p.

Le due condotte descritte dal legislatore, infatti, sono perfettamente equivalenti dal punto di vista giuridico, nel senso che ognuna di esse integra pienamente il fatto tipico; ma da ciò non è possibile trarre la conseguenza di una radicale alterità, con il rischio *in limine* di legittimare un concorso formale fra fattispecie considerate a tutti gli effetti autonome.

Le due condotte, indicate attraverso concetti piuttosto generali, sembrano almeno parzialmente sovrapponibili, ma conservano comunque un ambito di applicazione autonomo: se da un lato non è possibile infatti considerare l'intervento senza diritto come una mera azione prodromica all'alterazione del sistema, sia poiché può integrare autonomamente una condotta tipica di frode informatica sia poiché l'alterazione del funzionamento può essere realizzata con modalità varie che prescindono da esso[66], dall'altra è pur vero che spesso il reato *de quo* si sostanzia in una condotta "composita" che si sviluppa attraverso momenti alterativi e intervenivi, che non è possibile scindere nettamente.

Ciò trova giustificazione nel fatto che il legislatore, temendo di lasciare senza una protezione penale condotte che era complesso descrivere in termini esaustivi, ha preferito utilizzare una descrizione sovrabbondante del fatto tipico, anche al fine di ricomprendervi tutte le condotte *latu sensu* manipolative che ai fini di profitto possono colpire un elaboratore, con uno sguardo attento anche ai futuri sviluppi dell'informatica[67]. Si tratta in conclusione di due facce della stessa medaglia, due condotte sicuramente indipendenti e autonomamente sussistenti (essendo pacifico che basta la commissione di una per configurare il fatto tipico) che però conducono al medesimo risultato, ovvero la punibilità ex art. 640-ter c.p..

I tentativi di parte della dottrina di separare nettamente le due condotte

[65] C. Pecorella, *op.cit*., pag. 90
[66] Per esempio un'alterazione di *hardware* non implica intervento su dati o programmi.
[67] M. Romani - D. Liakopoulos, *op.cit*., pag. 248

potrebbero condurre ad equivocare la volontà del legislatore, il quale, avendo scelto di indicarle nella medesima disposizione, aveva senza dubbio ravvisato una vicinanza fra le stesse, per lo meno in termini di offensività. Inoltre si concretizzerebbe il rischio di escludere dall'ambito applicativo della fattispecie condotte che potrebbero validamente essere sanzionate[68]: una concettualizzazione dogmatica rigida, troppo votata alla precisazione delle condotte, finisce per allontanarsi dalla realtà concreta e ha come effetto anche una perdita di quell'elasticità che deve sempre caratterizzare le disposizioni, anche quelle penali. A maggior ragione in un settore a rapidissimo sviluppo come quello delle tecnologie informatiche e telematiche, nel quale è necessario conservare una buona dose di fluidità e plasmabilità delle formulazioni normative per poter far fronte alle nuove esigenze di tutela; a tali istanze ben risponde anche la formulazione delle due condotte attraverso concetti precisi e tecnici ma pur sempre generali.

L'altro rischio, portando alle estreme conseguenze il ragionamento, è di indurre il giudice a sanzionare due volte il medesimo comportamento materiale, poiché potrebbe rilevare la autonoma sussistenza di due comportamenti radicalmente differenti, in concorso formale.

Anche sulla qualità delle condotte si registra qualche contrasto in dottrina: Fondaroli le considera indeterminate, poiché la norma non descrive in maniera sufficientemente analitica le caratteristiche e modalità dell'alterazione; Mucciarelli invece sostiene che l'indicazione fornita dal legislatore all'art. 640-ter c.p. sia più precisa rispetto alla generica richiesta di "artifizi e raggiri" nella truffa tradizionale[69].

Al riguardo si ritiene che sia molto difficile dire in astratto se la previsione normativa nella frode informatica sia più o meno determinata rispetto alla

[68] Per esempio, considerando l'intervento senza diritto come condotta meramente preparatoria e dipendente dall'alterazione di sistema, il giudice potrebbe non rilevare la sussistenza della condotta tipica, nemmeno allo stadio del tentativo, nel comportamento di un soggetto che non si sostanzia in una piena alterazione del funzionamento del sistema, arrestandosi invece (per fatti e circostanze non dipendenti dalla sua volontà) ad un mero intervento su dati o programmi senza altre conseguenze.

[69] Nel primo senso D. Fondaroli, "*La tutela penale dei 'beni informatici'*", in Diritto dell'informazione e dell'informatica, 1996, pag. 307; per la seconda opinione vedi F. Mucciarelli, "*Commento dell'art. 10 della l. 23/12/1993, n. 547*, in Legislazione penale, 1996, 137, C. Pecorella, *op.cit*., pag. 87 e S. Logroscino, articolo citato *supra*.

fattispecie di cui all'art. 640 c.p.: molto dipende in entrambi i casi dalla capacità dell'operatore del diritto di dare sostanza alle condotte attraverso un percorso argomentativo coerente e preciso, che nel primo caso tenga conto soprattutto della configurazione informatica della condotta (la ricchezza e completezza dal punto di vista tecnico-informatico sono un importante ausilio per la determinatezza) e nel secondo nell'idoneità concretamente ingannevole degli artifizi e raggiri.

La giurisprudenza, pur con qualche distinguo, ha generalmente condiviso il secondo orientamento con riguardo alla qualità delle condotte previste dall'art. 640-ter: si è così sostenuto che le stesse sono alternative e distinte, pur ribadendo l'unicità di reato[70]. È sufficiente che l'azione posta in essere dall'agente integri gli estremi di una delle due condotte tipizzate per aversi frode informatica. Spesso si ritiene che la seconda condotta operi in via suppletiva rispetto alla prima: l'"intervento senza diritto" viene configurato quasi come condotta a forma libera e quindi viene utilizzata in tutte quelle ipotesi in cui non si riesce a dimostrare tecnicamente l'"alterazione del funzionamento" di un sistema.

Nella maggior parte delle pronunce però l'attenzione dei giudici, soprattutto di legittimità, si è concentrata sull'oggetto materiale della condotta (il sistema informatico o telematico), descrivendolo in maniera molto precisa e lasciando più ampia la descrizione della condotta, concepita quasi come libera[71].

2.3.1. *Alterazione del funzionamento di un sistema informatico o telematico*

Il primo tipo di intervento fraudolento si sostanzia in "*un'alterazione in qualsiasi modo del funzionamento di un sistema informatico o telematico".*

Si tratta di una modificazione dello svolgimento regolare di un processo di elaborazione, lettura, emissione o trasmissione di dati: dato che la disposizione fa riferimento in maniera piuttosto generica al "funzionamento" del sistema, si

[70] Tribunale Torino, 30/09/2002, in Diritto dell'informatica, 2003, 322; Cass. Pen., sez. II, sent. n. 9891 del 24/02/2011 – 11/03/2011; Cass. Pen., sez. II, sent. n. n. 13475 del 22/03/2013.

[71] Si può trovare un'attenta riflessione sul concetto di "*sistema informatico*" in Cass. Pen., Sez. VI, sent. n. 3067 del 14/12/1999, *Piersanti*, ripresa poi in altre pronunce come Cass. Pen. , Sez. II, sent. n. 13475 del 22/03/2013.

ritiene infatti che la modifica realizzata dall'agente possa colpire qualsiasi funzione svolta dall'elaboratore[72].

Per capire quando si ha alterazione, bisogna fare riferimento al risultato del processo che viene preventivato dal programmatore o dall'utilizzatore. Qualsiasi elaboratore elettronico, inserendo determinati comandi, viene programmato per svolgere una o più operazioni specifiche: ad un *input* corrisponde sempre un *output*. Ponendo in essere un'alterazione del funzionamento, l'agente modifica il processo informatico, facendo sì che l'elaboratore produca un risultato diverso rispetto a quello regolare. Tale condotta è quindi caratterizzata da una logica di manomissione delle modalità predeterminate di funzionamento di un sistema, a differenza della seconda condotta che è rivolta unicamente a "dati, informazioni o programmi" e non implica necessariamente una loro manomissione[73].

La modificazione può intervenire in una fase qualsiasi del processo di elaborazione, sia sugli "scopi" cui il sistema informatico è destinato sia sui contenuti dello stesso[74]. Può comportare, anche indirettamente, una manipolazione sia dei dati destinati a essere successivamente elaborati (manipolazione di *input*), sia delle istruzioni relative allo specifico trattamento a cui i dati stessi devono essere sottoposti (manipolazioni di programma), sia infine di dati già regolarmente elaborati ma che devono essere decodificati in un linguaggio intelligibile all'uomo (manipolazione di *output*)[75]. Avuto riguardo all'oggetto immediato sul quale ricade la condotta fraudolenta, si possono distinguere le manipolazioni di *software*, ossia quelle che incidono sulla componente logica del sistema, dalle manipolazioni di *hardware*[76], ovvero quelle che colpiscono la componente meccanica dello stesso.

Le più complesse dal punto di vista tecnico-informatico – e proprio per questo

---

[72] C. Pecorella, *op.cit*., pag. 82

[73] Vedi *infra* cap. II par. 3.2

[74] V. S. Destito, G. Dezzani, C. Santoriello, "*Il diritto penale delle nuove tecnologie*", Cedam, Padova, 2007.

[75] Esempi sono lo *Scavening* o *Trashing*, metodo per recuperare informazioni dagli scarti di un lavoro effettuato con l'elaboratore, e il *Data Leakage*, vera e propria rimozione di dati o copie di dati dal sistema del computer. C. Sarzana di S. Ippolito, *op.cit*., pag. 70-71

[76] La casistica di manipolazioni di *hardware* è molto scarsa, dato che richiedono notevoli capacità tecniche e la possibilità di accesso fisico al sistema; sono comunque condotte comprese nella fattispecie per completezza e precauzione di fronte alla molteplici modalità di aggressione a sistemi informatici

poste in essere per lo più da esperti del settore – sono le manipolazioni di programma, che possono essere realizzate in due modi: alterando alcuni passaggi logici previsti in un programma originale ovvero introducendo un programma diverso e ulteriore di "disturbo", appositamente predisposto dall'agente per realizzare l'indebito profitto[77]. Solamente la seconda di tali ipotesi rientra unanimemente nella condotta di "alterazione di funzionamento"; sulla prima si registrano più contrasti in dottrina, essendo da molti considerata più propriamente un "intervento senza diritto su programma".

Esempi di manipolazioni di programma si riscontrano soprattutto nel settore bancario: famosi sono i casi di "*Rounding-down fraud*" (frode dell'arrotondamento verso il basso) in cui vengono manipolati i programmi che servono per il calcolo degli interessi passivi dovuti dalle banche ai clienti, oppure la "*Salami technique*", tecnica con cui vengono sottratte piccole somme di denaro provenienti da un gran numero di accrediti, di modo tale che le variazioni non risultino immediatamente percepibili da parte dei clienti.

Molto diffusa anche a livello privato è la tecnica del "*Trojan horse"* (cavallo di Troia) che implica l'inserimento surrettizio di un programma malevolo all'interno dell'elaboratore attraverso l'installazione di un programma utile: il *malware* è nascosto in esso e, quando il programma d'appoggio viene lanciato, inizia ad operare anch'esso in background, senza che l'utilizzatore se ne accorga.

Negli ultimi anni le più pericolose e dannose tecniche di attacco informatico sfruttano la rete Internet con i suoi miliardi di utenti e le possibilità di anonimato che offre: una di queste è l'APT, *Advanced Persistant Threats*.

In esso gli *hackers* in primis individuano gli utenti bersaglio attraverso i vari social network, spesso rintracciando fra loro dipendenti di grandi società o istituti di credito. Tentano poi di introdursi nei sistemi di questi soggetti attraverso l'invio e-mail di "phishing"[78] che consentano di infettare la macchina con un *malware* autoinstallante. A questo punto il sistema informatico aziendale risulta compromesso: l'attacco prosegue cercando di sottrarre loro le credenziali

[77] Può essere impiegato un programma che si limita ad impartire istruzioni diverse da quelle preventivate dal titolare del sistema oppure può essere azionato un programma "contrario al sistema", che altera, blocca o paralizza parzialmente o totalmente le funzioni regolari. C. Pecorella, *op.cit*.

[78] Il fenomeno del "Phishing" sarà analizzato *infra* cap. V par. 3.

di amministratore del dominio o altri dati sensibili e di inserire nel sistema *utilities* malevoli che permettano di costruire una vera e propria struttura di controllo parallela, in grado di impartire comandi, intercettare e-mail e acquisire informazioni su denaro e procedure. Ma soprattutto, tale attacco è in grado di mantenere la persistenza all'interno del sistema e di resistere anche nel momento in cui qualche parte della struttura illegale venga scoperta[79]: tale caratteristica, assieme all'altissimo livello tecnologico, lo rendono molto più pericoloso e più difficile da individuare e bloccare rispetto ai tradizionali virus e malware. Con questa sofisticata tecnica sono stati attaccati istituti bancari come "JP Morgan Chase", importanti catene di negozi (Home Depot, Benetton) o istituti assicurativi (Anthem)[80].

Pregi della modalità d'azione in commento sono sicuramente l'ampiezza ed elasticità del dettato normativo, che hanno permesso sviluppi inaspettati nell'applicazione dello stesso: recentemente è stata ravvisata dalla Suprema Corte un'alterazione di sistema informatico nel fatto di modificare il funzionamento di un apparecchio da gioco in luogo aperto al pubblico, al fine di non versare l'imposta stabilita dalla legge per le c.d. slot machine[81].

2.3.2. *Intervento senza diritto su dati, informazioni o programmi*

La seconda condotta è costituita da un "*intervento senza diritto con qualsiasi modalità su dati, informazioni o programmi".*

Si tratta di una forma d'interferenza, diretta o indiretta, con un processo di elaborazione, rivolta a destinatari precisamente individuati (solo dati, informazioni o programmi) ma che può avvenire in forma libera. Il legislatore ha

[79] Una recente ricerca ha evidenziato come un intervistato su cinque riferisca che la propria azienda ha subito un attacco di minaccia persistente avanzata; inoltre il 94% degli intervistati ritiene che gli attacchi APT rappresentano una minaccia reale per la sicurezza della propria nazione e per la stabilità economica, ma che, malgrado questa consapevolezza, la maggior parte della aziende sta implementando tecnologie inefficaci per la propria tutela.
Ricerca ISACA sulla sicurezza informatica commissionata da Trend Micro Inc. http://www.trendmicro.it/newsroom/pr/la-nuova-ricerca-isaca-sulla-sicurezza-informatica-commissionata-da-trend-micro-rivela-che-unazienda-su-cinque-ha-subito-un-attacco-apt-/

[80] Rapporto Clusit 2015, su attacchi informatici avvenuti nel 2014

[81] Cass. Pen., sez. V, sent. n. 27135 del 19/03/2010; Cass. Pen., sez. II, sent. n. 18909 del 30/04/2013; per un approfondimento dell'orientamento in commento, vedi *infra*.

scelto di delimitare tale forma d'azione solo dal punto di vista dell'oggetto immediato su cui ricade la condotta e con l'inciso "senza diritto"[82]: le concrete modalità dell'azione sono *ex se* irrilevanti per la configurazione della fattispecie. L'azione produce una modificazione del contenuto o della destinazione di tali dati, informazioni o programmi: anche in questo caso quindi, a seconda della fase in cui interviene, potrà colpire gli *input*[83], gli *output* o i programmi stessi.

La differenza fondamentale rispetto alla prima condotta si rinviene nell'assenza di una modifica strutturale del funzionamento dell'elaboratore: la giurisprudenza, in maniera molto chiara, parla di condotta illecita "*intensiva ma non alterativa del sistema informatico o telematico*", sottolineando così come l'agente ottenga il proprio profitto con altrui danno senza intaccare la regolarità delle operazioni compiute dal sistema.

Anzi, nella maggior parte dei casi è necessario che il sistema funzioni per poterne trarre profitto: si pensi alle frodi all'I.N.P.S. o all'Agenzia delle Entrate in cui operatori con la disponibilità dei terminali dell'Istituto inseriscono dati falsi relativi alla situazione contributiva di determinate imprese per non far figurare il mancato pagamento di oneri previdenziali od assistenziali, o perfino far risultare crediti d'imposta non reali o riscuotere illegittimamente ratei pensionistici[84].

Oltre ai programmi, oggetto e limite della manipolazione sono i dati e le informazioni: se i dati e i programmi fanno riferimento alle componenti logiche di un sistema, ossia alle rappresentazioni di informazioni o istruzioni codificate in una forma non intelligibile in via immediata, le informazioni sembrano a prima vista esulare dal contesto applicativo, data la loro immediata percettibilità e la possibilità di manipolazione solo nel momento in cui vengono convertite in "dati"[85]. L'inserimento di tale oggetto materiale permette di estendere i confini applicativi della fattispecie, eliminando qualsiasi tipo di dubbio in rapporto a quelle condotte di disturbo realizzate al di fuori del processo di elaborazione in

[82] Per un approfondimento sull'inciso "*senza diritto*" vedi *infra* cap. II par. 4.

[83] Nel c.d. *Data Diddling* vengono trasformati dei dati prima del loro inserimento o durante l'inserimento stesso

[84] Vedi fra i tanti: Trib. Roma, 20 giugno 1985, *Testa ed altri*; Cass. Pen., sez. II, sent. 6958 del 25/01/2011, Cass. Pen., sez. II, sent. n. 13475 del 22/03/2013.

[85] Proprio in virtù del fatto che la condotta fraudolenta si rivolge ad un elaboratore elettronico, molti legislatori (ad es. c.p. austriaco e c.p. greco) stranieri hanno menzionato come oggetto materiale solo i dati e i programmi, a volte ritenendo fuorviante il riferimento alle informazioni. C. Pecorella, *op.cit*.

senso stretto, ma comunque aventi ad oggetto informazioni "pertinenti" al sistema, o perché ancora da sottoporre a trattamento informatico o perché provenienti da una elaborazione già avvenuta. Modificando un'informazione prima che venga elaborata dal sistema, i dati poi introdotti sono irrimediabilmente falsati e si creano le condizioni per la causazione di un risultato irregolare; qualora l'informazione venga modificata dopo che è già stata sottoposta alla elaborazione informatica, si avrà una manipolazione di *output*, sanzionabile ex art. 640-ter c.p. solo nei limiti in cui la stessa conservi un nesso di pertinenzialità con un sistema informatico o telematico[86]. Deve trattarsi inoltre di una condotta che sarebbe sanzionabile a titolo di truffa se il documento non provenisse da un'elaborazione informatica: la peculiarità dell'elaborazione informatica del documento non deve diventare motivo per ampliare illimitatamente la rilevanza penale delle condotte, pena la violazione della *ratio* stessa che ha ispirato l'introduzione dell'art. 640-ter c.p.[87].
Conclusivamente bisogna sottolineare come, a livello pratico, quest'ultima distinzione abbia poca rilevanza, poiché la sanzione prevista dall'art. 640 c.p. è la medesima di quella prevista per la frode informatica.

2.4 L'inciso "*senza diritto*"

La seconda condotta prevista dall'art. 640-ter c.p. è caratterizzata dal legislatore prevalentemente con l'inciso "*senza diritto*", trattandosi per il resto di semplice "intervento con qualsiasi modalità".
Fin dai primi commenti, molti Autori hanno rilevato la forte equivocità di tale espressione[88], a prima vista incoerente con la struttura del reato. In effetti, è difficile individuarne la natura giuridica: se si riferisse l'espressione alla posizione del soggetto rispetto al sistema nel suo complesso, richiedendo per la configurazione dell'illecito la mancanza del diritto di intervenire, l'operatore del

[86] Si potrà trattare quindi di una manipolazione di output destinati successivamente ad un'altra elaborazione informatica oppure di manipolazioni "strumentali", commesse per mascherare o nascondere un profitto già acquisito operando all'interno del sistema.
[87] C. Pecorella, *op.cit*.
[88] G. Pica, *op.cit.*, pag. 146; Alma - Perroni, "*Riflessioni sull'attuazione delle norme a tutela dei sistemi informatici"*, in Diritto e procedura penale, 1997,n. 4, pag. 506

sistema – per definizione autorizzato ad accedervi – sarebbe sempre esente da responsabilità rispetto alla seconda modalità di condotta[89]. Si creerebbe così un "cortocircuito normativo", dato che proprio l'art. 640-ter c.p. prevede che l'abuso della qualità di operatore di sistema costituisca il presupposto per l'applicazione della aggravante prevista al secondo comma del medesimo.

Altro significato attribuibile a tale locuzione risulta dal riferimento alla concreta operazione posta in essere, la quale avverrebbe appunto "senza diritto"; l'agente avrebbe il pieno diritto di accedere al sistema e agire sullo stesso. Quindi si include nel raggio d'azione della norma quel soggetto che ha la facoltà giuridica di accedere al sistema e/o di mantenervisi, ma pone in essere una condotta per la quale non è autorizzato o che non gli è stata richiesta.

Argomentando rispetto al primo significato, si desume che non è possibile dare alla locuzione il significato di "assenza della facoltà giuridica di intervento" sul sistema *tout court*: l'abuso della qualità di operatore del sistema costituisce una circostanza aggravante del reato in questione, prevista nel medesimo art. 640-ter, che si configura perciò nell'ipotesi base come reato comune. La condotta in astratto può essere posta in essere da un *extraneus*, soggetto che non ha nessun legame giuridico o fattuale con il sistema attaccato, come da un *intraneus*, individuo che ha sia le competenze tecniche sia la possibilità materiale di agire su un determinato sistema (e beninteso spesso così avviene).

Se si interpretasse la locuzione "senza diritto" in termini assoluti, il rischio di escludere dall'applicazione della fattispecie tutti coloro che agiscono su dati e software a scopo di illecito profitto avendo il diritto di intervenire su di essi sarebbe piuttosto concreto: con la conseguenza di creare delle brecce d'impunità nell'ordinamento proprio in quei casi in cui è più facile la commissione dell'illecito, data la materiale disponibilità dei sistemi[90].

La prima limitazione necessaria per coerenza sistematica va fatta riferendo l'inciso "senza diritto" alla legittimazione a compiere uno specifico intervento sul sistema. Agisce "senza diritto" colui che compie una determinata attività sui dati contenuti in un elaboratore senza essere a ciò autorizzato da una norma

[89] A. Manna, "*Artifici e raggiri on-line: la truffa contrattuale, il falso informatico e l'abuso dei mezzi di pagamento elettronici*", in Diritto dell'informazione e dell'informatica, 2002, 955.
[90] G. Pica, *op.cit.*

positiva o da una norma contrattuale, ovvero da altre fonti[91].

Anche in questi termini però, l'inciso non assume un pieno ed autonomo significato: non si capisce come potrebbe configurarsi una condotta manipolativa di sistema che non sia "senza diritto". Il fatto stesso di procurarsi (o tentare di procurarsi) un profitto ingiusto con altrui danno, manipolando un processo rispetto al risultato regolare connota la condotta di illiceità: non è possibile concepire un'azione di questo tipo posta in essere "con diritto".

Pertanto, la seconda condotta prevista dall'art. 640-ter c.p. configura una fattispecie "a forma libera"[92]: qualsiasi condotta manipolativa di dati, informazioni o programmi attraverso la quale l'agente si procuri un profitto illecito con danno altrui realizza gli estremi del fatto tipico, ricorrendone gli altri presupposti. Si tratta di una locuzione che nulla aggiunge ad una condotta che trova la propria nota di offensività nella lesione del patrimonio, consumata o tentata. La disposizione è costruita come reato d'evento, e come tale va interpretata ed applicata: la condotta manipolativa che ha come destinatario immediato l'elaboratore elettronico o i contenuti di esso è pur sempre volta all'ottenimento di un vantaggio patrimoniale.

Sotto questo profilo, si può considerare l'inciso "senza diritto" un'ipotesi di antigiuridicità non reale ma apparente, richiamando semplicemente l'assenza di facoltà giuridica di agire ex art. 51 c.p.[93].

Peraltro, la scelta della locuzione "*senza diritto*" operata dal legislatore non appare affatto casuale. Si tratta di un'espressione diversa da altre utilizzate sempre in ambito informatico: per esempio, nel caso di danneggiamento informatico (art. 635-bis c.p.), il legislatore ha scelto di parlare di "altruità" di dati o programmi informatici.

Ciò è ben spiegabile sulla base in primo luogo dell'analisi della struttura delle due fattispecie. La struttura della frode informatica rispecchia la sua oggettività

---

[91] V. S. Destito, G. Dezzani, C. Santoriello, "*Il diritto penale delle nuove tecnologie*", Padova, 2007 in S. Logroscino, "*La frode informatica quale autonoma figura di reato rispetto al delitto di truffa*", su Altalex.

[92] S. Logroscino, *supra*. Per la giurisprudenza, Cass. Pen, sez. II, sent. 9891 del 11/03/2011.

[93] F. Mantovani, "*Diritto penale, Parte speciale – Delitti contro il patrimonio*", Cedam, Padova, 2002, pag. 210; C. Del Re, "*La frode informatica*", ed. Polistampa, 2009.

giuridica di delitto contro il patrimonio[94]: la tutela penale interviene solo nel momento in cui vi è una concreta (o un rischio effettivo di) lesione al patrimonio altrui con indebito vantaggio patrimoniale per l'agente.

Il delitto di danneggiamento informatico, invece, tutela in primis l'integrità dei sistemi informatici e dei dati e programmi in essi conservati; è per questo che la tutela penale opera in tal caso ad uno stadio anteriore, non essendo necessario il verificarsi di un danno patrimoniale. La norma è costruita come reato di mera condotta: l'offensività del fatto risiede tutta nella azione di distruzione, cancellazione, soppressione di dati o programmi informatici altrui.

In secondo luogo bisogna rilevare che non sempre le condotte fraudolente realizzate in ambito informatico volte all'ottenimento di un profitto illecito con altrui danno, hanno come oggetto immediato una "cosa altrui". Vi possono essere casi in cui la condotta ricade su dati che sono nella legittima disponibilità dell'agente o sui quali l'agente stesso può esercitare un diritto di godimento. La scelta di riferirsi all'intervento indebito piuttosto che all'altruità dell'oggetto materiale utilizzata nelle ipotesi di danneggiamento informatico permette di ampliare e precisare la portata applicativa della norma, includendovi quelle fattispecie in cui l'intervento colpisce dati, informazioni o programmi propri dell'agente o su cui l'agente ha legittimamente la facoltà di agire (si pensi all'operatore INPS o al funzionario dell'Agenzia delle Entrate che per definizione lavorano con dati, informazioni o programmi altrui; o recentemente al concessionario di apparecchi per l'intrattenimento con vincita, il quale pone in essere una condotta manipolativa su cose nella propria legittima disponibilità).

Inoltre tale scelta legislativa permette di ricomprendere nell'alveo dell'art. 640-ter c.p. anche le ipotesi in cui l'accesso in sé considerato avviene in maniera legittima ma vengono utilizzate credenziali altrui per realizzare operazioni indebite nel sistema: in questi casi, semplicemente vengono sfruttate a fini di profitto personale informazioni riservate di accesso di un altro soggetto.

Per poter applicare la fattispecie in commento, è necessario spostare l'attenzione dal momento dell'utilizzo dei dati altrui a quello della esecuzione

[94] Per un analisi del rapporto fra la fattispecie in commento e la truffa vedi cap. II par. 2.

dell'operazione economica[95]: l'intervento non autorizzato avviene sui dati che sono già contenuti nel sistema, non su quelli utilizzati per l'accesso, consumandosi nel momento in cui avviene l'illegittima sottrazione patrimoniale altrui e il consequenziale proprio profitto[96].

Ad oggi quindi è possibile includere a pieno titolo questo tipo di fattispecie nell'"intervento senza diritto" di cui all'art. 640-ter comma 1 c.p., a maggior ragione dopo che nel 2013 è stata introdotta l'aggravante di cui al comma terzo. Nel momento in cui avviene una sottrazione patrimoniale utilizzando dati sensibili altrui, ossia con "*furto o utilizzo indebito di identità digitale*", non solo si può configurare una frode informatica, ma sarà anche aggravata sia nel trattamento sanzionatorio sia nella perseguibilità (è prevista infatti la perseguibilità d'ufficio)[97].

2.5 L'oggetto materiale della condotta

Per chiarire l'effettiva portata applicativa delle condotte incriminate dall'art. 640-ter c.p. occorre individuare in maniera precisa la nozione e le caratteristiche, da un lato, del "*sistema informatico o telematico*" su cui viene compiuta la manipolazione e dall'altro dei "*dati, informazioni o programmi*" sui quali il soggetto attivo interviene indebitamente. Il legislatore ha sì cercato di precisare le condotte tipiche rispetto alla previsione rinvenibile nella truffa tradizionale, nella quale erano state inserite locuzioni ampie prettamente lasciate all'interpretazione dell'operatore del diritto[98]: ma è pur vero che si tratta

[95] C. Pecorella, *op.cit.*

[96] Si pensi ad una sottrazione di denaro operata accedendo all'*Home Banking* altrui con l'ausilio delle credenziali di tale soggetto: l'accesso è in sé legittimo ma avviene da parte di un soggetto che non è a ciò legittimato. Il momento consumativo del reato si rinviene nell'ottenimento del vantaggio patrimoniale attraverso la sottrazione fraudolenta.

[97] Per un'analisi della nuova aggravante del 2013, cap. III par. 2.

[98] La dottrina maggioritaria considera la truffa reato a forma vincolata, per la contemporanea presenza di più elementi caratterizzanti la condotta, ovvero artifici e raggiri e induzione in errore cui segue casualmente il profitto con danno; G. Fiandaca – E. Musco, *op.cit.*, F. Mantovani, *op.cit*. Peraltro, l'evoluzione della giurisprudenza nell'applicazione dell'art. 640 c.p. ha fornito un'interpretazione sempre più ampia di tali elementi: già negli anni '80 si rinvengono varie pronunce in cui si considera artifizio o raggiro "*ogni espediente subdolo, posto in essere per indurre taluno in errore*": Cass. Pen., 25/03/1982, *Mazzaferro*, Cass. Pen., 12/12/1983, *Barberini*. Perciò non è importante tanto definire esattamente i confini dei concetti di artifizi e

di due condotte che possono realizzarsi espressamente "*in qualsiasi modo*" e "*con qualsiasi modalità*", quindi oggetti ampi la cui caratterizzazione e delimitazione risulta fondamentale.

Quando il legislatore deve normare un settore a rapidissimo sviluppo come quello delle tecnologie informatiche, è obbligato a contemperare esigenze opposte: sicuramente deve ricorrere a termini tecnici per descrivere in modo puntuale il fenomeno, che proprio sul piano tecnico si caratterizza e si differenzia dalle ipotesi di reato tradizionali, ma deve comunque impiegare termini che siano il più possibile "sganciati" dalla tecnologia (ossia *tecnology-indipendent*) per evitare che le norme stesse diventino presto superate e quindi incapaci di stare al passo con lo sviluppo del settore dando una risposta sanzionatoria effettiva[99].

Proprio per evitare il rischio di obsolescenza delle fattispecie delittuose derivante dalla cristallizzazione dei concetti, il legislatore italiano – in linea con la maggior parte degli ordinamenti di *civil law* – ha scelto di non fornire alcuna definizione legale dei termini tecnici inseriti nell'art. 640-ter c.p., lasciando così alla dottrina e alla giurisprudenza il compito di concretizzarli[100].

Invero, la disposizione italiana presenta anche alcune peculiarità rispetto alle scelte normative di molti altri Paesi[101], sia con il riferimento – a prima vista quasi generico – al "*sistema informatico o telematico*" anziché al "processo di elaborazione dati", sia nel menzionare pure le "informazioni" assieme ai "dati e programmi". Innanzitutto, per quanto attiene alla nozione di "sistema informatico", bisogna rilevare come si tratti di un concetto piuttosto generale e

---

raggiri, poiché gli stessi possono consistere in qualsiasi rappresentazione falsata della realtà che abbia l'attitudine concreta ad indurre in errore un soggetto. La giurisprudenza, criticata da parte della dottrina, recentemente si è spinta oltre, ravvisando la truffa altresì in ipotesi in cui la condotta dell'agente si sostanzia in un'omissione: vedi fra le tante, Cass. Pen., sez. II, sent. n. 39905 del 2/11/2005 (ud. 11/10/2005), Cass. Pen., sez. II, sent. 41717 del 14/10/2009, in cui si considerano integrati gli artifici o raggiri nel silenzio maliziosamente serbato su alcune circostanze da colui che abbia il dovere di farle conoscere; Cass. Pen., sez. II, sent. n. 22692 del 13/05/2008, in cui si ravvisa il medesimo elemento tipico nel silenzio serbato nei confronti dell'I.N.P.S. circa il fatto della sopravvenuta sospensione della potestà genitoriale.

[99] C. Pecorella, *op.cit*., pag. 69

[100] C. Pecorella, *op.cit*.

[101] Ad esempio, il codice penale tedesco, il codice penale austriaco, il codice penale portoghese ed infine il codice penale svizzero individuano l'oggetto materiale nel processo di elaborazione dei dati o nel trattamento automatico di dati; il codice penale giapponese e quello danese caratterizzano in maniera ancora più specifica tale processo, considerando rilevante solo quello che avviene in maniera elettronica. Così C. Pecorella, *op.cit.*

duttile, in grado di ricomprendere qualsiasi sistema adibito al trattamento automatizzato di dati che si avvalga dell'informatica: l'informazione, oggetto di trattamento, viene codificata nel linguaggio accessibile alla macchina diventando *input*, dato pronto per l'elaborazione automatizzata, dalla quale scaturisce poi l'*output*, il dato elaborato che viene tradotto nuovamente nel linguaggio intellegibile all'uomo. Alla funzione di registrazione-memorizzazione elettronica di dati intesi quali "*rappresentazioni elementari di un fatto*" si affianca la funzione complementare e fondamentale di elaborazione-organizzazione logica di tali dati in insiemi più o meno estesi, costituenti "informazioni"[102].

I primi commentatori si interrogarono su quali dimensioni di complessità dovesse avere un "sistema" per essere considerato tale: alcuni Autori infatti rilevarono che per "sistema" si dovesse intendere solo un complesso di attrezzature dotate di un grado di strutturazione e complessità superiori a quelle di un *personal computer* [103].

Già G. Pica criticò tale impostazione, sottolineando l'ingiustificato restringimento dell'ambito applicativo della fattispecie che essa avrebbe comportato, vanificandone l'efficacia. Invero, anche la Relazione ministeriale che accompagnava il disegno di legge[104] si esprimeva in termini piuttosto ampi, riferendosi ai "*sistemi informatici di qualunque tipo e dimensione, comprendendo in tale accezione sia i sistemi di scrittura o di automazione d'ufficio ad uso individuale o particolare, sia complessi sistemi di elaborazione dati in grado di fornire servizi e potenza di calcolo a migliaia di utenti, sull'intero territorio nazionale od anche oltre i confini del Paese*": risulta perciò che il legislatore del '93 avesse piena consapevolezza sia dell'esigenza di tutelare anche i sistemi individuali (personal computer)[105] ormai diffusissimi, sia delle potenzialità dell'informatica e della conseguente necessità di tenere presenti sviluppi in quel momento forse nemmeno immaginabili.

Altro aspetto che denota l'estrema lungimiranza della scelta italiana è il puro riferimento all'informatica come metodo di funzionamento dell'elaboratore,

---

[102] G. Stalla, "*L'accesso abusivo ad un sistema informatico o telematico*", reperibile su: www.penale.it/commenti/stalla01_html

[103] G. D'Aietti, in Borruso ed altri, "*Profili penali dell'informatica*", Giuffré, Milano, 1994

[104] Camera dei Deputati, XI Legislatura, Disegno di Legge n. 2773.

[105] G. Pica, *op.cit.*, pag. 23

evitando di precisare la tecnica concretamente impiegata per il trattamento dei dati: l'elaborazione infatti può essere elettronica, magnetica, ottica, elettrochimica, ma il richiamo ad una specifica pratica avrebbe reso presto inapplicabile la norma.

La giurisprudenza risalente della Corte di Cassazione ha offerto un importante contributo[106], in base al quale è sistema informatico ogni "*complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo attraverso l'utilizzazione (anche parziale) di tecnologie informatiche.*

Queste ultime sono caratterizzate dalla compresenza di tre elementi funzionali:

a) *la registrazione o memorizzazione, "attraverso un'attività di "codificazione" e "decodificazione", per mezzo di impulsi elettronici e su supporti adeguati, di "dati" rappresentati attraverso simboli (bit), in combinazioni diverse";*
b) *"l'elaborazione automatica" da parte della macchina dei dati così registrati o memorizzati;*
c) *l'organizzazione di tali dati "secondo una logica che consenta loro di esprimere un particolare significato per l'utente"* .

La funzione della macchina-computer ad organizzare ed elaborare dati sulla base di un certo programma *(software*) ed in vista di finalità eterogenee costituisce elemento discretivo essenziale, consentendo di distinguere ciò che è *"informatico*" da ciò che è invece solamente *"elettronico*"[107].

L'espressione "sistema informatico" si rivela così estremamente ampia ed in grado di affrancarsi dalla necessità di un elaboratore inteso in senso tradizionale (computer composto da *case*, monitor ed eventuali periferiche), per essere applicata ogniqualvolta si è in presenza di una condotta manipolativa su un apparecchio che compie in maniera automatizzata una funzione organizzativa ed elaborativa di contenuti, a prescindere dalla dimensione o

[106] Cass. Pen., sez. VI, sent. n. 3067 del 14/12/1999, *Piersanti*.

[107] Così, ad esempio, il videoregistratore, il lettore di CD (sempre che non siano connessi ad un computer con funzione di masterizzazione o elaborazione di immagini e suoni), i dispositivi che presiedono all'attivazione dei sistemi di sicurezza sulle auto (come l'airbag, o l'ABS), certi elettrodomestici a tecnologia digitale sempre più diffusi nelle nostre case, non possono considerarsi – proprio perché inidonei alla elaborazione ed organizzazione di dati nel senso che si è detto – "sistemi informatici", quanto solamente apparati elettronici; G. Stalla, "*L'accesso abusivo ad un sistema informatico o telematico*"

dalla tipologia: elemento chiave è l'autonomia di funzionamento, una volta impartite le istruzioni in linguaggio informatico.

Già nelle prime applicazioni dell'art. 640-ter c.p., i giudici di legittimità hanno mostrato di aderire all'interpretazione lata dell'oggetto materiale diffusasi presto nei tribunali: è stata così riconosciuta la natura di "sistema informatico" anche alla rete telefonica fissa, sia per la modalità di trasmissione dei flussi di conversazioni, sia per l'utilizzo delle linee per il flusso dei cc.dd. dati esterni alle conversazioni[108].

In pochi anni così si è assistito ad una crescente "smaterializzazione" dei sistemi, che si sono liberati di tutte quelle periferiche superflue rispetto alla elaborazione di contenuti in senso stretto ed hanno assunto la connotazione di meri processori di dati. Grazie allo sviluppo delle nanotecnologie, la prospettiva si è invertita: non vi è più una specifica macchina da identificare come sistema informatico per le funzioni che svolge, ma vi è solo un micro-processore che può esso stesso essere implementato in qualsivoglia dispositivo o apparecchiatura utile all'uomo. Perciò qualsiasi tipo di strumento nel quale viene inserito un processore in grado di trattare in maniera automatizzata degli *input* per creare nuovi *output* può considerarsi sistema che opera con metodo informatico. Con la Convenzione di Budapest del 2001 è stata finalmente pattuita – seppur ai soli fini della convenzione medesima – a livello internazionale una definizione di "sistema informatico", anch'essa piuttosto ampia: all'art. 1 viene così descritta "*qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati*".

In quest'ottica diventa sistema informatico anche una carta a microprocessore che, a differenza delle comuni carte magnetiche, incorpora un piccolissimo computer, registrato su una minuscola piastra di silicio (c.d. *microchip*): queste carte di nuova generazione hanno ormai sostituito quasi completamente le carte a banda magnetica e richiedono un'attenzione particolare da parte dell'operatore del diritto, chiamato ad applicare la norma giuridica adeguata al caso concreto scegliendo fra la fattispecie di frode informatica e la fattispecie

[108] Cass. Pen., sez. VI, sent. n. 3067 del 14/12/1999.

specificamente introdotta per sanzionare l'indebito utilizzo di carta di credito o pagamento ovvero di qualsiasi documento analogo (art. 55 comma IX d.lgs. 231/2007)[109].

Sono riconducibili alla nozione di "sistema informatico" anche gli apparecchi elettronici che forniscono beni o servizi (distributori automatici di sigarette, il singolo sportello Bancomat, macchine per fotocopie azionate con tessera magnetica, nonché tutti gli apparecchi automatici oggi affidati alla gestione di un elaboratore, quindi anche gli *smartphone*): si tratta pur sempre di macchine al cui interno avviene un trattamento informatico di dati, in quanto il processore in esse installato è in grado – grazie alle istruzioni impartite – di vagliare la legittimazione dell'utente a ricevere la prestazione, elaborare il comando ricevuto ed eventualmente modificare, cancellare o aggiungere funzioni personalizzate.

La estrema versatilità del concetto in esame ha permesso ai giudici di legittimità di utilizzare la fattispecie di frode informatica anche in casi di alterazione del funzionamento di apparecchi elettronici destinati a "giochi di abilità" o al gioco di intrattenimento senza vincite e trasformati in *slot machine*, al fine di conseguire un profitto non tassando i relativi proventi[110].

Accanto a questi sistemi che potremmo definire "isolati" per la loro capacità di svolgere la funzione per la quale sono stati programmati in maniera autosufficiente, esistono sistemi "complessi", risultanti dalla interconnessione tra elaboratori situati anche a notevole distanza tra loro attraverso le vie di telecomunicazione, ovvero attraverso una rete elettrica o mediante un sistema di trasmissione via etere[111]: tali sistemi sono creati per trasmettere e ricevere informazioni in tempo reale in luoghi anche molto distanti e proprio questa è la funzione ulteriore rispetto al sistema informatico non connesso. L'elemento che consente di ravvisare un sistema *"telematico*" in luogo di un mero dispositivo di trasmissione a distanza di segnali (come il telefono o il fax) è dato proprio dal

[109] Il problema del rapporto fra le due disposizioni verrà affrontato *infra* cap. IV par. 1.

[110] Cass. Pen., sez. V, sent. n. 27135 del 19/03/2010; Cass. Pen., sez. II, sent. n. 18909 del 30/04/2013.

[111] Il riferimento principale va alla rete Internet che conta quasi 3 miliardi di soggetti connessi nel mondo ma sono comprese anche le reti Intranet, reti aziendali private molto di dimensioni contenute.

fatto che ad essere collegati tra loro sono due o più sistemi informatici. La scelta italiana di menzionare espressamente anche questa versione più evoluta di sistemi appare condivisibile, poiché permette di risolvere ogni dubbio in relazione alla operatività della frode informatica anche nei loro confronti, evitando di compromettere in pochi anni l'utilità e la certezza dell'intervento legislativo; inoltre, permette di includere nel raggio d'azione della fattispecie tutte quelle condotte alterative che non incidono direttamente sul funzionamento del singolo sistema informatico ma colpiscono il funzionamento di una rete stessa, magari determinando un black-out dei collegamenti attraverso l'utilizzo di un server remoto oppure creando dei collegamenti vietati.

In questo modo la Corte di Cassazione ha ricompreso nell'alveo di tali sistemi non solo sistemi di trasmissione e condivisione dati di grandi enti pubblici o imprese private (si pensi per es. al sistema di gestione dati di INPS, il sistema di gestione di Poste Italiane, i sistemi di gestione bancari o assicurativi, recentemente anche il sistema di Expo), ma anche le "centraline telefoniche", poiché tecnicamente il trasporto delle informazioni avviene in forma cifrata attraverso impulsi elettronici (i bit), con procedimento automatizzato di codificazione e decodificazione che abilita l'utilizzo delle linee per la chiamata solo di determinate utenze: sia la rete telefonica, sia il centralino della singola filiale costituiscono impianti che si avvalgono in modo integrato di tecnologie informatiche[112]. Non rileva il livello di prestazioni che sono in grado di fornire: per questo motivo non pare accoglibile quell'orientamento che vorrebbe riconoscere l'appartenenza al *genus* di sistemi informatici solo a quei dispositivi elettronici e similari che sono collegati, direttamente (*on-line*) o indirettamente (*off-line*), con elaboratori più sofisticati[113].

[112] Cass. Pen., sez. VI, sent. n. 3065 del 4/10/1999, *De Vecchis*: nel caso di specie, l'agente, utilizzando il sistema telefonico fisso installato nella filiale Telecom dove operava, riusciva ad ottenere collegamenti internazionali vietati, eludendo il blocco appositamente predisposto sulla rete attraverso una veloce ed ininterrotta digitazione di numeri telefonici, in parte corrispondenti a quelli per i quali il centralino era abilitato, in parte esteri. In questo modo la Telecom veniva esposta debitoriamente nei confronti dei corrispondenti organismi esteri autorizzati all'esercizio telefonico.

[113] Si tratta di una delimitazione che non trova nessun riscontro normativo e che non risponde alla *ratio* della fattispecie, strutturata come reato d'evento in cui il fulcro dell'offesa cade sul conseguimento del profitto illecito attraverso l'uso fraudolento di un sistema informatico. C. Pecorella, *op.cit.*

La giurisprudenza ha altresì ricondotto allo schema della frode informatica l'uso di un apparecchio telefonico clonato, individuando il sistema telematico nella rete di telefonia mobile: la clonazione è un'operazione che consente di addebitare ad un'utenza telefonica i costi delle chiamate effettuate a mezzo di un altro apparecchio cellulare, assegnando abusivamente il numero di utenza e la stringa seriale ad un diverso cellulare appositamente riprogrammato. Si tratta di un'attività diretta ad alterare surrettiziamente il funzionamento del sistema telematico della società di gestione, che riconosce ed addebita all'utente titolare del telefono clonato il traffico effettuato da colui che si avvantaggia della clonazione[114].

Bisogna comunque sottolineare come sia irrilevante dal punto di vista sostanziale precisare con esattezza se il sistema aggredito sia informatico o telematico, in quanto i due termini indicano concetti che spesso si integrano a vicenda. Questa interrelazione si manifesta a livello formale attraverso un'endiadi tutelata indistintamente in ogni disposizione che specificamente li riguarda: la distinzione assume rilevanza dal punto di vista delle forme di aggressione che possono essere anche diverse nei confronti dell'uno o dell'altro sistema.

L'oggetto materiale della seconda condotta fraudolenta prevista dall'art. 640-ter c.p. sono le componenti logiche del sistema, ossia i "*dati, informazioni o programmi*", contenuti nello stesso. Si tratta di una formula alquanto singolare nel panorama internazionale, determinata forse dalla preoccupazione di dare una risposta sanzionatoria a qualsiasi tipologia di manomissione di contenuti informatici, conosciuta e non. Molti legislatori stranieri hanno scelto formule più tecniche, ossia annoverando esclusivamente i dati e i programmi e ritenendo superflua la menzione delle informazioni, sulla base della circostanza che la condotta fraudolenta si rivolge ad un sistema informatico anziché ad una persona; altri hanno preferito il riferimento più sintetico ed esaustivo alla

[114] "*L'utilizzazione di un apparecchio radiomobile clonato costituisce frode informatica […] che si realizza con la manipolazione del sistema informatico telefonico mediante l'immissione nello stesso di dati falsi che consentono un ingiusto profitto in danno del sistema informatico medesimo*"; Cass. Pen., sez. II, 21 dicembre 2001, in *Foro ambrosiano*, 2002, 180; L. Cuomo, R. Razzante, "*La disciplina dei reati informatici*", Giappichelli, 2007.

categoria generale delle “informazioni”, nella quale si fanno rientrare anche quelle gestite elettronicamente.

Il legislatore italiano non ha inteso operare un distinguo tecnico fra le varie nozioni, ma si è limitato a creare una formula ampia ed omnicomprensiva di qualsiasi elemento registrato in un sistema informatico, quale che sia il suo significato intrinseco, in modo da evitare vuoti di tutela derivanti da un’incompleta formulazione.

Autorevole dottrina ha tentato di individuare le differenze dal punto di vista concettuale sussistenti fra i vari elementi della locuzione, per definire un ambito applicativo proprio di ciascuno: la menzione del programma accanto ai dati e alle informazioni è apparsa subito pleonastica, essendo il programma stesso costituito da un insieme di dati, specificamente una sequenza di istruzioni assemblate per ottenere dalla macchina precise operazioni prestabilite. L’utilità di tale elemento può essere rinvenuta sul piano pratico, nella chiarezza ed esaustività che in tal modo assume il dettato normativo e nella possibilità di incriminare condotte nelle quali magari appare evidente l’intervento indebito sul programma ma non si riesce ad individuare il singolo dato colpito, aggiunto o rimosso.

Dati ed informazioni invece non sono sinonimi, poiché designano due realtà ben differenti: benché il primo concetto non sia univoco, si propende per lo più a considerare come dati solo quelle rappresentazioni di informazioni che sono già state codificate nel linguaggio comprensibile alla macchina, introdotte nella stessa come *input*, soggette ad organizzazione ed elaborazione automatizzata, dalla quale scaturisce il nuovo dato elaborato, l’*output*. Correlativamente, le informazioni sono tali proprio in quanto siano direttamente comprensibili dall’utente: è possibile quindi intenderle in due accezioni, sia come dati cognitivi desumibili da un supporto materiale, sia come correlazioni logiche di dati, redatte e organizzate in un linguaggio che permette anche all’utente della macchina di attribuire loro un univoco e determinato significato.

Nel primo caso, il riferimento alle informazioni permette di ricomprendere nell’ambito delle frodi informatiche le manipolazioni di c.d. “documenti originari”, casi nei quali l’informazione viene direttamente letta e tradotta dalla macchina

attraverso particolari tecnologie (scanner, lettore ottico), senza che intervenga l'operato e l'errore umano: tali ipotesi sarebbero confluite in linea teorica nell'ambito della truffa, poiché l'informazione è contenuta su un supporto materiale intelligibile all'uomo, ma l'assenza di controlli da parte di una persona incaricata di trasferire il contenuto su supporti informatici avrebbe reso impossibile individuare un'induzione in errore. Grazie a tale interpretazione, la norma in commento potrebbe svolgere un ruolo fondamentale anche con riguardo alle condotte manipolative che intervengono su supporti tradizionali, in una fase precedente alla traduzione delle informazioni sotto forma di dati.

Un altro caso in cui ha rilevanza la menzione delle informazioni è quello della manipolazione di "output stampati", risultati dell'elaborazione non più codificati in dati ma riportati su documenti o supporti che permettano la lettura da parte dell'uomo: se tali output, invece che essere destinati direttamente all'uomo, fossero trattati dallo stesso sistema informatico che li ha elaborati o da un altro, la manomissione degli stessi comporterebbe un risultato irregolare, tale da causare il profitto illecito e il danno altrui. Alla luce di questa interpretazione, l'inclusione delle informazioni fra gli oggetti materiali sui quali può ricadere l'intervento senza diritto appare opportuna, poiché permette di individuare una frode informatica anche in quelle condotte interventive che si svolgono al di fuori del processo di elaborazione in senso stretto ma che hanno sostanzialmente natura informatica: ciò che rileva non è tanto l'intelligibilità del dato informativo da parte dell'uomo, ma il fatto stesso che esso rimane nel circuito dell'elaborazione informatica e dal sistema viene trattato, pur non essendo un dato o un programma.

Accogliendo la seconda accezione nella quale vengono proposte le "informazioni", l'ampliamento del raggio d'azione della frode informatica è più contenuto: vengono prese in considerazione tutte quelle condotte fraudolente che, lasciando di per sé inalterati i dati raccolti in memoria, ne modificano le interconnessioni, falsando il risultato dell'elaborazione[115].

La giurisprudenza non ha dato particolare attenzione all'analisi di tale nozione, facendo propendere per l'assunto che si tratti di tre concetti che il legislatore ha

[115] M. Romani, D. Liakopoulos, "*La globalizzazione telematica*", Giuffré, 2009, pag. 241

deciso di trattare congiuntamente per creare una nozione unica, omnicomprensiva e – forse un po' troppo – generale, per indicare qualsiasi condotta interventiva su un contenuto informatico: in varie sentenze infatti, la Cassazione ha semplicemente ricostruito la seconda condotta come reato a forma libera che si concretizza in una "*illecita condotta intensiva ma non alterativa del sistema informatico o telematico*", la quale ha come obiettivo materiale un qualsiasi contenuto dello stesso[116].

Sulla base di queste promesse, la Suprema Corte ha rinvenuto una frode informatica nell'utilizzo abusivo di codici d'accesso di terzi comunque ottenuti, dei quali si è venuti in possesso all'insaputa o contro la volontà del legittimo possessore, per operare uno spostamento patrimoniale con illecito profitto per sé e danno al titolare del conto collegato alle predette credenziali[117].

Il continuo perfezionamento e raffinamento delle tecniche d'intrusione rende assai difficile la stesura di una normativa che preveda *una tantum* l'intera fenomenologia del reato informatico: per questo motivo la scelta delle nozioni più generali appare la più adeguata, anche se forse la complessa da maneggiare.

2.6 L'evento del reato

Dopo aver chiarito le condotte che possono integrare la fattispecie di cui all'art. 640-ter c.p., bisogna analizzare gli eventi in senso naturalistico che vi sono eziologicamente connessi e capire quando può ritenersi consumato il reato.

La disposizione si esprime nei medesimi termini della fattispecie tradizionale di truffa, richiedendo che le condotte fraudolente causino un "*ingiusto profitto con altrui danno*". Sulla base di tale scelta contenutistica, già nel 1999 la Suprema Corte ha sottolineato che per la frode informatica può essere utilizzata l'elaborazione giurisprudenziale relativa alla truffa, giacché gli elementi

[116] Da ultimo Cass. Pen., sez. II, sent. n. 13475 del 22/03/2013.
[117] Cass. Pen., sez. II, sent. n. 9891 del 11/03/2011

costitutivi delle due fattispecie sono quasi totalmente sovrapponibili[118].

Vi è però una differenza fondamentale con l'art. 640 c.p.: essendo quest'ultima una fattispecie bilaterale necessaria, in cui il soggetto frodato coopera con l'agente sulla base di un inganno, deve verificarsi anche un atto di disposizione patrimoniale da parte dello stesso che permetta all'agente di ottenere l'illecito profitto. Costui non necessariamente coincide con il soggetto passivo del reato (per es. può essere indotto in errore l'operatore dello sportello bancario, mentre il soggetto passivo sarà il titolare del conto corrente depauperato).

Parte della dottrina, inoltre, isola come evento a sé stante anche l'induzione in errore di un soggetto.

Nel caso di frode informatica, invece, la condotta manipolativa ha come bersaglio il funzionamento dell'elaboratore o i contenuti informatici dello stesso: da questa premessa l'orientamento più consolidato sia in dottrina sia in giurisprudenza sostiene che non sia possibile rinvenire l'induzione in errore di "taluno", data l'inesistenza di una relazione interpersonale nei momenti di azione e consumazione. Poi però l'univocità si frammenta in posizioni alquanto eterogenee: alcuni, soprattutto in dottrina, sostengono che la disposizione vada integrata a livello ermeneutico (come già avviene nel caso di truffa) con un evento intermedio che rimane quindi implicito[119]. Altri invece sono di opposto avviso e affermano che l'interprete non debba rinvenire alcun evento inespresso come l'atto di disposizione patrimoniale: l'agente pone in essere una condotta direttamente sulla macchina, dalla quale deriverebbe causalmente il profitto per sé o per terzi con danno altrui[120]. Alcuni Autori poi hanno cercato di

---

[118] "*Il reato di frode informatica ha la medesima struttura, e quindi i medesimi elementi costitutivi, della truffa, dalla quale si distingue solamente perché l'attività fraudolenta dell'agente investe non la persona (soggetto passivo), bensì il sistema informatico (significativa è la mancanza del requisito della "induzione in errore") che gli pertiene.* […] *L'elaborazione giurisprudenziale relativa alla truffa - che si attaglia, mutatis mutandis, per i motivi anzidetti, anche al reato di frode informatica - è pervenuta alle conclusioni che il reato si consuma nel momento in cui l'agente consegue l'ingiusto profitto, con correlativo danno patrimoniale altrui*". Cass. Pen., sez. VI, sent. n. 3065 del 4/10/1999, , "*De Vecchis*"; ribadito poi in Cass. Pen. sent. n. 4576 del 5/02/2004; Cass. Pen. sent. n. 8755 del 26/02/2009; infine, Cass. Pen. sez. II, sent. n. 18909 del 10/04/2013.

[119] È altresì discusso in cosa consista tale evento intermedio: Pecorella lo individua nel risultato irregolare del processo di elaborazione (*supra* cap. II par. 2), Mucciarelli in una disposizione patrimoniale posta in essere dal sistema informatico o telematico.

[120] Anche nei Paesi in cui la previsione normativa richiede espressamente come evento intermedio la causazione di un risultato irregolare del processo di elaborazione dati non è

mediare, rinvenendo sul piano logico-interpretativo tale evento implicito intermedio come risultato del processo diverso da quello preventivato dal programmatore o utente legittimo del sistema, anche se non si tratta di un evento naturalistico in senso stretto.

Si è già avuto modo di analizzare la scelta del legislatore italiano di non richiedere espressamente la causazione di un risultato irregolare nel processo di elaborazione e trattamento dati e i rischi connessi a tale opzione[121]. Dal canto suo, la giurisprudenza maggioritaria spesso non si dilunga nel dimostrare un evento intermedio, soffermando piuttosto l'attenzione sulla configurazione delle condotte manipolativa o interventiva, sull'oggetto materiale[122] e sull'evento naturalistico "tangibile" (danno e profitto). Si ha l'impressione che, per l'applicazione della disposizione in commento, ciò che avviene all'interno dell'elaboratore non sia *ex se* rilevante perché non ha un reale effetto al di fuori della macchina: diventa rilevante solo nel momento in cui conduce causalmente all'illecito profitto con altrui danno.

A prescindere dalla sussistenza o meno di un evento implicito, dottrina e giurisprudenza sono pressoché unanimi nel ritenere che, per la configurazione della fattispecie, è necessario sussistano cumulativamente[123] sia un profitto ingiusto sia un danno ad un terzo. Tuttavia, mentre si registra un sostanziale accordo sull'estensione delle elaborazioni in tema di truffa alle analoghe questioni poste dalla fattispecie di frode informatica, lo stesso non può dirsi sul percorso argomentativo che conduce a tale conclusione. Da un lato, la giurisprudenza e parte della dottrina basano il proprio *iter* logico-giuridico sull'identità di struttura fra la fattispecie tradizionale di truffa e la frode informatica[124]; dall'altro, alcuni Autori motivano l'attinenza alla frode informatica

---

richiesta la cooperazione artificiosa della vittima: si ha semplicemente una sequenza causale più simile a quella prevista nella truffa, tuttavia rimane sempre escluso l'intervento attivo della vittima, colpita solo alla fine come destinatario passivo. C. Pecorella, *op.cit*.

[121] Cap. II, par. 2.

[122] Varie pronunce hanno analizzato la nozione di "*sistema informatico o telematico*": Cass. Pen., sez. VI, sent. n. 3067 del 14/12/1999, *Piersanti*; Cass. Pen., sez. II, sent. n. 13475 del 22/03/2013.

[123] "*In tema di truffa, la realizzazione del profitto e quella del danno debbono essere contestuali, trattandosi di dati fra loro collegati in modo da costituire due aspetti della stessa realtà*", Cass. Pen., sez. II, sent. n. 27950 del 18/06/2008.

[124] Vedi nota n. 117

delle elaborazioni teoriche riguardanti la truffa con la scelta legislativa del medesimo modulo descrittivo in riferimento ai soli eventi naturalistici. In altri termini, secondo quest'ultimo orientamento, le due disposizioni sono strutturalmente differenti ma è possibile applicare anche alla frode informatica i risultati dell'elaborazione dottrinale e giurisprudenziale in tema di *eventus damni* della truffa, per il fatto che il legislatore del '93 ha ripreso esattamente il medesimo modulo descrittivo dell'art. 640 c.p. rispetto a questi elementi, richiedendo un ingiusto profitto dell'agente o di altri con altrui danno come conseguenza della condotta fraudolenta[125].

Entrambi tali elementi possono essere intesi in senso oggettivo o soggettivo: appare evidente come la soluzione debba essere comune, trattandosi in sostanza di decidere l'interpretazione della *ratio* giustificatrice della norma in esame.

La parte di dottrina che utilizza una nozione di profitto oggettivamente intesa rimane saldamente ancorata all'idea della necessaria patrimonialità dello stesso: con ciò però non si intende più il patrimonio nel senso statico di accumulo di beni materiali o denaro, ma l'accezione del termine è dinamica e dematerializzata, includendo tutti quei rapporti giuridici od attività cui è sotteso un valore economicamente stimabile[126]. Altro orientamento, invece, utilizza una nozione di profitto estremamente ampia e avulsa dal dato patrimoniale, includendovi anche tutti quegli interessi aventi un mero valore affettivo per il titolare[127]. Entrambe le teorie trovano a proprio sostegno serie argomentazioni e sono in astratto condivisibili: ma ragioni di collocazione sistematica e strutturali delle fattispecie penali di frode, unite al valore delle singole scelte terminologiche compiute dal legislatore penale, fanno propendere per la prima

---

[125] L. Alesiani, "*Il momento consumativo del delitto di frode informatica: indicazioni contraddittorie della Cassazione*" in Cass. Pen., n. 1/2001, pag. 491; G. Marini, "*Digesto delle opere penalistiche,* (voce) *Truffa (Frode informatica)"*, Torino, 2006.

[126] G. Pica, *op.cit*., pag. 156; per la concezione dinamica del patrimonio, C. Castronovo, "*Manuale di diritto privato europeo*, Vol. 2", Milano, Giuffré.

[127] Così ad es. Cass. Pen., sez. II, sent. n. 7730 del 3/04/1986: "*In tema di truffa, il profitto, a differenza del danno che deve sempre avere natura patrimoniale, può non avere carattere economico, potendo anche consistere nel soddisfacimento di qualsiasi interesse, sia pure soltanto psicologico o morale*". Cass. Pen., Sez. Unite, 16/12/1998, in Giur. It., 2000. In tal senso anche D. D'Agostini, "*Diritto penale dell'informatica – Dai computer crimes alla Digital Forensic*", Esperta, Forlì, 2007, pag. 37.

di esse con qualche adattamento.

Sia la truffa sia la frode informatica sono collocate nel titolo del codice penale dedicato alle lesioni del patrimonio e condividono tale bene giuridico: la dimensione in cui la condotta viene realizzata è tutta patrimoniale, sia nel momento del danno sia nel momento del profitto. Sarebbe incoerente positivizzare la disposizione a tutela di un bene giuridico determinato e dotato di una propria consistenza misurabile, per poi dilatarlo a livello interpretativo fino a ricomprendere utilità che non hanno nessuna connotazione patrimonialistica, consistendo in meri interessi di natura psicologica o affettiva, come tali non stimabili. Inoltre il sistema penale prevede specifiche ipotesi di tutela "anticipata" rispetto alle frodi, come l'art. 615-ter c.p. che punisce il mero accesso abusivo ad un sistema informatico o telematico protetto o l'art. 615-quater c.p. che interviene a reprimere la mera detenzione e diffusione abusiva di codici d'accesso ai medesimi sistemi. Si tratta di fattispecie profondamente diverse dai delitti di frode: sono state collocate fra i "*Delitti contro la persona*", nel titolo che raggruppa le fattispecie incriminatrici di quelle condotte che ledono o minacciano di ledere interessi che ineriscono direttamente alla persona umana (per esempio la riservatezza in ambito informatico o il domicilio informatico, inteso come proiezione in ambito virtuale del domicilio fisico). La tutela anticipata deriva dalla costruzione delle fattispecie come reati di mera condotta[128]: per la consumazione è sufficiente che l'agente ponga in essere le condotte tipizzate, a nulla rilevando se si è verificato o meno un evento di danno. Infatti il bene giuridico relativo alla persona viene leso già nel momento in cui la condotta è posta in essere.

Anche il dato terminologico può avvalorare la teoria del profitto economico-patrimoniale: il diritto penale è dominato dal principio di tassatività-determinatezza, che esige – più che in altri settori dell'ordinamento – precisione nella redazione delle fattispecie incriminatrici e attenzione nella scelta dei singoli termini usati. Il legislatore storico, consapevole di ciò, ha usato vari

[128] Nell'art. 615-quater c.p. la soglia della punibilità è ancor più anticipata, configurandosi come reato di pericolo, dato che sanziona il mero possesso o la mera detenzione di codici d'accesso ottenuti abusivamente: in altri termini, l'ordinamento presume che possa sussistere un pericolo per il titolari di detti codici quando vengono acquisiti in maniera abusiva, quindi interviene con la sanzione.

termini per indicare situazioni vantaggiose ("denaro", "profitto", "utilità", "vantaggio"), graduati in base alla concretezza e alla valenza patrimoniale, a testimonianza del riferimento a realtà distinte: se avesse voluto estendere agli interessi soggettivi l'applicazione delle fattispecie di frode, avrebbe potuto utilizzare la nozione di "utilità", sola o assieme a quella di "profitto".

Per profitto illecito quindi s'intende qualsivoglia tipo di vantaggio economicamente valutabile, anche quindi un semplice risparmio di spesa[129], ottenuto in maniera non lecita: nessuna disposizione dell'ordinamento o pattuizione contrattuale consente all'agente di ottenere quel dato vantaggio o di conseguirlo attraverso quelle modalità. Ovviamente la disposizione violata può avere anche natura extra-penale: può trattarsi della violazione di una norma civile, amministrativa, tributaria, previdenziale. Si tratta quindi di una nozione volutamente ampia ed elastica, in grado di stare al passo con lo sviluppo socio-economico-tecnologico, e di includere qualsiasi tipo di vantaggio che l'agente ha ottenuto *sine causa* o *contra iure* e che la collettività (e quindi il legislatore) ritiene meritevole di presidio penale. Solo attraverso un concetto così generale l'interprete può riempire concretamente di significato la locuzione ed essere pronto a fronteggiare qualsiasi nuova forma di abuso informatico, anche quelle totalmente prive di un sostrato materiale ovvero più impensabili.

Una delle ultime applicazioni della Corte di Cassazione dell'art. 640-ter c.p. riguarda ipotesi di mancato versamento dell'imposta dovuta sugli apparecchi da gioco a vincita aleatoria, grazie alla modifica fraudolenta del *chip* contenuto nelle stesse[130]: la Suprema Corte ha così ritenuto di poter declinare l'ampia portata applicativa della norma verso la tutela dell'Erario statale, danneggiato da tale condotta fraudolenta e individuando conseguentemente il profitto

[129] La nozione di risparmio di spesa presuppone "*un ricavo introitato e non decurtato dei costi che si sarebbero dovuti sostenere, vale a dire un risultato economico positivo: in altri termini, il risparmio di spesa rileva come "profitto ingiusto" non in termini assoluti, ma solo in termini relativi, ossia in relazione ad un ricavo introitato*", Cass. Ufficio del massimario, Rel. N. 41/14, orientamento di giurisprudenza, reperibile qui: http://www.cortedicassazione.it/cassazione-resources/resources/cms/documents/Relazione_pen_41_14.pdf

[130] Su tale interpretazione nell'ambito della truffa *ex* art. 640 c.p., cfr. Cass. 17 gennaio 1957, in *Giust. pen.,* 1957, II, 458 per cui "*non è necessario che il profitto perseguito dall'agente abbia carattere economico, neppure in forma mediata, ben potendo esso consistere nel soddisfacimento di un bisogno di qualsiasi genere, anche soltanto psicolgico o morale"*; Cass. Pen., sez. V, sent. n. 27135 del 19/03/2010 e Cass. Pen., sez. II, sent. n. 18909 del 10/04/2013: *infra.*

ingiusto in un mancato esborso dell'imposta dovuta da parte del concessionario.

Si è già avuto modo di sottolineare come non manchi una parte della giurisprudenza, avallata anche dai giudici di legittimità, che ammette – sia in relazione alla truffa sia in relazione alla frode informatica – la rilevanza anche di una "*qualsiasi soddisfazione o piacere*" di tipo affettivo o morale "*che l'agente si riprometta di conseguire dalla propria condotta criminosa"*[131]: oltre alle considerazioni svolte precedentemente, che conducono a rifiutare tale concezione, essa pone difficoltà dal punto di vista della quantificazione sia del profitto sia nel danno. Inoltre nell'ambito della frode informatica appare di dubbia realizzazione pratica, giacché l'agente pone in essere una condotta fraudolenta sulla macchina che purtuttavia conduca in via mediata ed ultimativa ad un'offesa al patrimonio; mette le proprie conoscenze tecniche al servizio del vantaggio economico che vuole raggiungere. Sia i sistemi informatici singoli sia i sistemi telematici connessi permettono la circolazione di innumerevoli risorse, pressoché tutte caratterizzate dalla valutabilità dal punto di vista economico: il mondo virtuale è per definizione avulso da qualsiasi dimensione strettamente personale, affettiva o morale; quindi concepire una condotta fraudolenta che colpisca un elaboratore e crei esclusivamente un vantaggio dal punto di vista morale o affettivo è molto difficile se non impossibile[132]. Anche le condotte di *hacking* e *cracking* volte a frodare meri dati o informazioni in sistemi informatici di grande imprese o sui *social network* possono comportare vantaggi economicamente valutabili, dato che spesso si tratta di risorse in sé poco importanti ma dall'alto valore di mercato (per esempio in termini di mancato lucro cessante)[133]: negli ultimi anni si sta assistendo ad una marcata

[131] Cass. Pen., sez. III, sent. n. 23798 del 24/05/2012 - 15/06/2012; in materia di truffa, Cass. Pen., Sez. Unite, 16/12/1998, in Giur. It., 2000; S. Logroscino, *art.cit*. Altalex; in senso contrario con riferimento alla frode informatica, G. Marini, "*Digesto delle opere penalistiche,* (voce) *Truffa (Frode informatica)",* Torino, 2006.

[132] Senza contare che la disposizione in esame è stata collocata fra i "Delitti contro il patrimonio" come la truffa, quindi è quasi un controsenso cercare di individuare nel profitto un entità esclusivamente non patrimoniale.

[133] Ad esempio, nel 2014 è stato violato il sistema informatico di Benetton e sono stati sottratti illecitamente vari bozzetti della collezione 0-12;gli indumenti sono stati così replicati e finiti in vendita in Siria. Rapporto Clusit 2015, pag. 18

Non vi è dubbio che si configuri il profitto ingiusto con altrui danno anche se sono stati sottratti meri disegni.

patrimonializzazione dei dati personali del consumatore, l'acquisizione dei quali è oggetto di sempre maggiore interesse da parte delle imprese, tanto che alcuni in dottrina parlano di "oro digitale"[134]. Anche i meri dati inerenti ad una persona, i suoi gusti, i suoi interessi, assumono oggi in Internet un valore commerciale importante, poiché permettono alle imprese di orientare la produzione e ampliare il proprio target: non stupisce quindi che possano avere un valore economico e che avveduta dottrina statunitense già qualche anno fa ha tentato di monetizzare il valore medio dei dati personali di un consumatore-tipo[135].

Come nella truffa, il profitto ingiusto può essere ottenuto "*per sé o per altri*": la norma non richiede che destinatario del profitto sia direttamente il soggetto agente, assumendo rilevanza penale anche l'ipotesi in cui il conseguimento del profitto sia riferibile a soggetti terzi rispetto al reo.

Anche per quanto concerne il concetto di "danno", facendo sempre riferimento alla truffa, si rinviene un'elaborazione teorica piuttosto ricca[136]. Secondo una prima tesi, più restrittiva, la norma si riferisce solo al "danno emergente": l'ordinamento penale è autonomo e governato dal principio di tassatività che impone un'interpretazione indipendente, da svolgersi in termini molto rigorosi rispetto al concetto di danno così come sviluppato in ambito civilistico. Altro orientamento, più vicino alle esigenze di tutela effettiva, sostiene che il concetto di danno va costruito anche grazie all'elaborazione teorica sviluppatasi in sede civile e ingloberebbe così sia il danno emergente sia il lucro cessante[137]. L'interpretazione sistematica permette così di includere nell'alveo della tutela ex art. 640-ter c.p. quelle ipotesi in cui vengono frodati dati, informazioni, programmi o risorse che considerati in sé stessi non comportano un sostanziale danno economico; il reale (e spesso ingente) danno deriva dal loro sfruttamento sul mercato o da una valutazione alla luce delle dinamiche di mercato. Tale interpretazione non violerebbe il principio di tassatività, poiché in tema di patrimonio il collegamento con il diritto civile non solo sarebbe ammissibile, ma

[134] P. Cipolla, "*Social network, furto d'identità e reati contro il patrimonio*" in Giur. merito, 2012, 12, par. 7.
[135] R. S. Murphy, "*Property rights in personal information*", 1996, in http://www.lexisnexis.com/
[136] L. Viola, "*Ingiusto profitto e danno altrui nella c.d. truffa contrattuale*", settembre 2003, su: http://www.diritto.it/articoli/penale/viola.html
[137] Cass. Pen., sez. II, sent. n. 37170 del 11/09/2013; Cass. Pen., sez. II, sent. n. 40790 del 23/10/2009; Cass. Pen., sez. II, sent. n. 10085 del 05/03/2008.

addirittura dovuto e, ad ogni modo, sarebbe giustificato da esigenze di tutela effettiva.

L'altro aspetto discusso in dottrina e giurisprudenza è la concezione del danno, giuridica o economica. Secondo la prima concezione, la tutela apprestata dall'ordinamento interviene in ogni caso di danno così come delimitato e definito dalla legge, che risponde ad istanze di protezione della collettività. Vengono così individuate ipotesi, soprattutto in ambito civile, in cui rileva altresì il danno non patrimoniale (morale ed esistenziale), inteso come lesione che afferisce alla dimensione affettiva, psicologica e relazionale della persona, il danno d'immagine o il danno da perdita di *chances*; la concezione economica del danno invece individua esclusivamente nel danno monetizzabile, *deminutio patrimonii* in senso stretto, quello meritevole di presidio civilistico e di conseguenza penalistico.

Partendo dal dato sistematico, le fattispecie di frode sono collocate nell'ambito dei "*Delitti contro il patrimonio*", quindi quelle fattispecie poste a tutela dell'insieme dei rapporti giuridico-economici facenti capo ad una persona, fisica o giuridica. Si è portati così ad optare per la concezione economica del danno, più in linea con la collocazione sistematica delle fattispecie, ed anche più rispondente alle esigenze sottese al principio di tassatività e determinatezza[138].

Tuttavia la concezione giuridica del danno può diventare un utile temperamento dei risvolti interpretativi più estremi cui la concezione economica potrebbe condurre: l'ordinamento deve apprestare una tutela effettiva anche nel caso di un danno economicamente poco incisivo in astratto (o poco incisivo per alcuni), ma rilevante se valutato nel contesto socio-economico-culturale in cui si verifica. In dottrina, pur registrandosi qualche isolata posizione contraria[139], la *communis opinio* è quella di esigere l'apprezzabilità economica del danno, non potendovi rientrare utilità di tipo strettamente personale: anche molta parte della

[138] La concezione soggettiva e giuridica di danno comporta il rischio di una illimitata estensione del concetto medesimo, potendo essere ricompresi in astratto tutti quei beni, materiali od immateriali, verso i quali la vittima sente un certo attaccamento di tipo emotivo o psicologico

[139] A. Di Tullio D'Elisiis, op.cit., che afferma che il "danno" può avere natura anche non patrimoniale.

giurisprudenza sembra orientata in questo senso[140].

Per la valutazione del danno occorre, quindi, procedere ad una considerazione individuale che, comunque, non può confondersi con una considerazione puramente soggettiva. Le condizioni soggettive della persona offesa devono diventare il faro guida per la valutazione della concreta incidenza della diminuzione patrimoniale: il dato economico perciò non può mancare, ma così interpretato diventa il punto di partenza per una valutazione più globale e realistica che colloca al centro dell'indagine la persona.

Tali considerazioni sono pienamente applicabili anche in ambito informatico: l'*an* del danno si configura in termini di decurtazione patrimoniale per il soggetto indirettamente colpito dalla condotta alterativa o interventiva dell'agente; il *quantum* va valutato anche tenendo in debito conto le condizioni personali, relazionali e sociali della persona offesa e le specificità di contesto in cui si consuma.

Da più parti in dottrina si è sottolineata la necessità di ripensare il concetto stesso di "patrimonio", slegandolo da una concezione prettamente "economica-materiale" per poterlo caratterizzare in termini "giuridici"[141]: potrebbero così rientrare nel concetto di profitto quei vantaggi "giuridici" che si traducono o saranno in futuro suscettibili di tradursi in un ingiusto accrescimento patrimoniale per il reo. Diventerebbe così "patrimonio" non solo ciò che ha un intrinseco valore economico, ma anche tutto ciò che può essere sfruttato economicamente a proprio vantaggio, vale a dire ogni entità – materiale o immateriale – che possiede una potenzialità di ritorno economico per il legittimo titolare: fra queste rientrano a pieno titolo anche i dati personali di ogni consumatore, che stanno vedendo crescere vertiginosamente l'interesse commerciale alla loro acquisizione. Questo tipo di concezione risponderebbe in maniera più efficace alle esigenze di tutela della persona emerse negli ultimi

[140] Cass. Pen., sez. II, sent. n. 12027 del 23/12/1997, *Marrosu*; la Suprema Corte si esprime in termini di perdita definitiva del bene economico da parte del soggetto passivo, intesa come effettiva *deminutio patrimonii* in Sez. Un. del 16/12/1998; vedi inoltre, Cass. Pen., sez. II, sent. n. 7730 del 28/07/1986 (ud. 3/04/1986); Cass., sez. V, sent. n. 16304 del 27/11/1989 (ud. 20/09/1989), in per cui "*il danno deve avere contenuto patrimoniale, deve concretizzarsi cioè in un detrimento del patrimonio*".

[141] G. Pica, *op.cit.*; G. Malgieri, "*Il furto d'identità digitale: una tutela patrimoniale della personalità*", in "*La giustizia penale nella rete*", di R. Flor, D. Falcinelli, S. Marcolini, ed. DiPLaP, 2014.

anni: soprattutto grazie alla diffusione massiccia dell'utilizzo di Internet e alla elezione dei *social network*, dei *blog* e delle *chat-rooms* come luoghi privilegiati per l'interazione umana, si sta assistendo ad una virtualizzazione della persona creata anche grazie all'ingegno della persona stessa, la quale ha la facoltà di sfruttare la propria identità virtuale come se fosse una maschera di sua "proprietà", che confluisce nel suo patrimonio come componente immateriale.
Quindi si può sostenere che anche i dati e le caratteristiche inerenti la persona possono diventare parte integrante del patrimonio di ogni soggetto, in primis poiché le imprese sono ormai arrivate a comprendere che disporre di determinate informazioni sui gusti e sulle preferenze dei consumatori significa avere enormi margini di guadagno; inoltre poiché la propria proiezione identitaria creata nella rete è anche prodotto dell'ingegno, e come tale può essere sfruttata a fini commerciali. Infatti anche gli stessi consumatori stanno iniziando a capire che possono scegliere se e come diffondere i propri dati identitari per guadagnare[142].
Del resto, anche nel "Progetto Pagliaro" di riforma del codice penale fu suggerita una riconsiderazione del concetto di "patrimonio" in termini più personalistici.
Il rischio di violazione del principio di stretta legalità che deve guidare e governare il sistema penale è dietro l'angolo: è necessario quindi adoperarsi per un'applicazione il più possibile rigorosa sia della nozione di "profitto" sia di quella di "danno", nella quale si richieda la prova concreta dell'incidenza sulla sfera di pertinenza del soggetto.

2.7 Il momento consumativo

Il dibattito sul momento consumativo del delitto di frode informatica deriva ontologicamente dalla scelta teorica effettuata riguardo ai concetti di "danno" e "profitto".

[142] Basti pensare a tutti quei siti internet in cui, compilando questionari o partecipando a discussioni o dibattiti, è possibile guadagnare denaro o accumulare punti che vengono poi trasformati in buoni sconto al raggiungimento di determinate soglie. Un esempio: it.mysurvey.com/

Accogliendo la concezione oggettiva-economica degli eventi naturalistici, il momento consumativo va individuato nella concreta *deminutio patrimonii* cui consegue la effettiva disponibilità del bene-profitto da parte dell'agente. Non avrebbe rilevanza il momento in cui è stata posta in essere la condotta manipolativa sull'elaboratore (che quindi può avvenire anche a notevole distanza) né il luogo in cui avviene l'evento informatico: quel che conta è l'effetto ultimo sul patrimonio del soggetto passivo e il consequenziale incremento del patrimonio dell'agente. Le elaborazioni dottrinali e giurisprudenziali in materia di truffa possono dare utili spunti: danno e profitto sono considerati "*due dati fra loro collegati in modo da costituire due aspetti della stessa realtà*"[143]. Bisogna cautamente adattare tale assunto formulato dalla Corte di Cassazione al contesto informatico, in cui spazio e tempo subiscono compressioni e dilatazioni anche notevoli: perciò può accadere che i due eventi non si verifichino in maniera simultanea. Infatti sono gli stessi giudici di legittimità che, in tema di momento consumativo della frode informatica, si allontanano dai risultati ermeneutici in materia di truffa, per individuarlo nel "*luogo di esecuzione della attività manipolatoria del sistema di elaborazione dei dati*"; solo in via subordinata ci si potrà rivolgere al luogo dove il profitto è stato conseguito[144].

La ricostruzione dell'evento in termini patrimoniali è quella che più fedelmente rispecchia la natura di reato di evento di danno della frode informatica: diversamente opinando, si finirebbe per anticipare la soglia della punibilità al momento della semplice probabilità di verificazione del pregiudizio, trasformando in via interpretativa la fattispecie in commento da reato di danno a reato di pericolo.

La concezione soggettiva del profitto e del danno non fornisce una risposta esaustiva rispetto alla problematica del *tempus* e del *locus commissi delicti*; invero, se il profitto e il danno dipendono precipuamente dal "sentire

[143] Cass. Pen., sez. II, sent. n. 27950 del 18/06/2008

[144] Cass. Pen., sez. III, sent. n. 23798 del 15/06/2012, ribadito nei *Principali orientamenti della Procura Generale sulla risoluzione dei contrasti*, a cura di Fulvio Baldi, reperibili al link: (http://www.procuracassazione.it/procuragenerale-resources/resources/cms/documents/PENALE_QAD_ORIENTAMENTI_CONTRASTI.pdf).
Contra v. Cass. Pen., sez. I, sent. n. 40303 del 27/05/2013 (dep. 27/09/2013), in materia di accesso abusivo ad un sistema informatico.

individuale", viene a mancare qualsiasi riferimento estrinseco e oggettivo per risolvere eventuali controversie di diritto sostanziale e processuale, ad esempio sulla prescrizione o sulla competenza. Il riferimento patrimoniale perciò si configura anche come elemento che conferisce concretezza e precisione temporale all'evento; le considerazioni di ordine soggettivo e psicologico potranno (e dovranno) caratterizzarlo e definirne la reale portata nella vita della persona offesa, ma non possono diventare l'esclusivo metro di giudizio.

Nonostante le aperture più recenti, le indicazione fornite dalla giurisprudenza maggioritaria vanno nella direzione di considerare consumato il delitto "*nel momento in cui l'agente consegue l'ingiusto profitto con correlativo danno patrimoniale altrui*"[145].

Anche la più recente giurisprudenza di legittimità si esprime proprio in favore di questa opzione interpretativa, ribadendo il principio suesposto, cionondimeno rilevando come siano intervenute pronunce anche della stessa Cassazione che "*hanno indicato quale criterio di collegamento della competenza il luogo di esecuzione della attività manipolatoria del sistema di elaborazione dei dati o il luogo di esecuzione della alterazione del funzionamento del sistema*"[146].

La Corte sottolinea come si sia trattato di casi nei quali l'attività fraudolenta del soggetto attivo si sovrapponeva dal punto di vista fenomenologico al conseguimento del profitto: perciò si trattava di una corrispondenza legata alle specifiche circostanze dei casi concreti e non basata su una regola di diritto.

Si ribadisce come il vero fulcro della tipizzazione normativa in base al quale individuare il momento consumativo e la competenza "*concerne precipuamente il conseguimento del profitto ingiusto, rispetto al quale si pongono in alternativa le strumentali condotte di alterazione del sistema informatico e di intervento, o accesso, abusivi, "senza diritto con qualsiasi modalità" (art. 640-ter c. 1 c.p.)*."

Tale assunto appare molto chiaro a livello teorico in varie pronunce, ma vi sono stati casi in cui gli stessi giudici di legittimità non hanno tratto da tale premessa le dovute conclusioni. Il riferimento corre alla sent. n. 3065 del 1999, nella quale la Corte di Cassazione prima stabilisce a chiare lettere che per aversi

[145] Cass. Pen., sez. VI, sent. 3065 del 04/10/1999, "*De Vecchis*"; Cass. Pen., sez. III, sent. n. 23798 del 15/06/2012; Cass. Pen., sez. I, sent. n. 46101 del 07/10-07/11/2014.
[146] Cass. Pen., sez. I, sent. n. 46101 del 07/10-07/11/2014.

consumazione del delitto di frode informatica è necessario che l'agente consegua materialmente l'ingiusto profitto e si verifichi il danno altrui; poi però, nel caso di specie, ritiene integrato il requisito del danno (e quindi consumato il reato) nella semplice esposizione debitoria della società colpita dalla condotta fraudolenta, a nulla rilevando che il materiale esborso non era ancora stato eseguito[147].

In altre sentenze, i giudici di legittimità sembrano a prima vista anticipare il momento consumativo, individuandolo già nell'intervento abusivo sui dati del sistema, che comporta l'alterazione del funzionamento[148]. Ma leggendo con più attenzione, emerge un quadro più complesso: nella sent. n. 6958 del 2001, la condotta posta in essere prevedeva l'inserimento di dati fiscali falsi nel sistema, con l'obiettivo di risultare titolari di benefici fiscali in realtà non dovuti. Quindi si trattava di una situazione in cui il mero inserimento di tali dati falsi configurava direttamente in capo all'agente il risparmio di spesa, con correlativo danno per l'Erario: non poteva richiedersi un materiale conseguimento di vantaggio patrimoniale, né la scoperta della falsificazione dei dati, dato che la definitività della situazione contributiva scaturiva direttamente dall'intervento modificativo sui contenuti del database.

A ben vedere, il problema risulta mal posto: le difficoltà di individuare il momento consumativo del reato derivano da una concezione puramente materiale del conseguimento del profitto e della causazione del danno. Lo sviluppo di questi elementi nell'ambito della teorizzazione in materia di truffa ha comportato che si ricercassero in maniera pressoché automatica gli stessi nella frode informatica come eventi naturalisticamente ben determinati, caratterizzati dalla riscontrabilità dal punto di vista empirico e dalla concreta possibilità di apprensione, pur trovandosi in un contesto dematerializzato.

A differenza di quanto avviene nella truffa, quando un *hacker* altera il

[147] Si trattava di un caso di collegamenti telefonici eseguiti abusivamente da dipendenti Telecom attraverso l'uso improprio dei sistemi di cui avevano la disponibilità per ragioni lavorative: la Corte ha ritenuto la sussistenza del reato di frode informatica, rinvenendo il conseguimento del profitto in ciascuno dei momenti in cui i dipendenti infedeli erano riusciti ad ottenere i collegamenti con l'estero, e il danno per Telecom S.p.A. nell'esposizione debitoria di quest'ultima nei confronti delle imprese che gestivano i servizi telefonici nei Paesi di destinazione delle telefonate.

[148] Cass. Pen., sez. II, sent. n. 6958 del 25/01/2001.

funzionamento di un sistema informatico o interviene senza diritto su dati o contenuti virtuali non sta intrattenendo una relazione con un'altra persona dalla quale subdolamente carpire un guadagno: la sua azione è diretta ad alterare il regolare processo di elaborazione svolto dalla macchina automatizzata e si confronta con il funzionamento della stessa, svolgendosi la condotta in una dimensione puramente virtuale. E proprio nella stessa dimensione puramente virtuale può realizzarsi il profitto: non è necessario per la configurazione della frode che l'agente abbia acquisito materialmente una somma di denaro o un bene né che la vittima abbia già subito l'esborso.

Ciò che veramente è fondamentale è la definitività della situazione in ambito informatico, ovverosia che un vantaggio misurabile dal punto di vista economico entri nella esclusiva sfera di disponibilità dell'agente (o del beneficiario da lui determinato) e che correlativamente il soggetto passivo registri una diminuzione del proprio patrimonio, a prescindere da un nesso spazio-temporale con la realtà empirica: la valutazione deve avvenire in termini esclusivamente informatici. Perciò può accadere che il momento di realizzazione della condotta e l'evento si sovrappongano: in altre parole può senza dubbio accadere che l'agente, nel momento stesso in cui pone in essere la condotta abusiva sul sistema, stia ottenendo il proprio vantaggio economico e stia causando un danno nella sfera patrimoniale del soggetto passivo[149].

Non si richiede che il tempo e luogo della condotta siano nettamente separati dal tempo e luogo dell'evento o che si riscontri un evento dotato di materialità: dal momento in cui il soggetto offeso perde la esclusiva disponibilità di una situazione patrimoniale favorevole e l'agente – o il terzo designato – acquisisce la facoltà esclusiva di disporre di un profitto, si configura l'evento bipolare che caratterizza la frode informatica, a prescindere dalla distanza spazio-temporale che li separa dalla condotta (distanza che financo può mancare).

Nel caso sopracitato, nel momento stesso in cui l'operatore inserisce fraudolentemente degli sgravi fiscali nel sistema informatico dell'Agenzia delle Entrate si verifica il profitto, poiché già da quel momento tale soggetto rende

[149] Proprio come accade quando vengono inseriti dati falsi in un sistema per ottenere qualche tipo di vantaggio patrimoniale.

diversa da come regolarmente dovrebbe essere – ergo si configura intervento senza diritto – una situazione contributiva, creando quindi una propria ed esclusiva disponibilità (o disponibilità esclusiva di beneficiari da lui scelti) di situazioni patrimoniali favorevoli acquisite abusivamente: il momento in cui, grazie ai controlli, viene scoperta la frode non è rilevante per la consumazione del reato.

Bisogna sempre tener presenti le peculiarità della dimensione virtuale, singola o in rete che sia, e in primis la dematerializzazione e l'anonimato delle azioni e degli eventi: nel mondo virtuale è complesso individuare il momento in cui un soggetto consegue un determinato vantaggio, se esso viene cercato comunque utilizzando le regole valide in un contesto materiale, dato che nella maggior parte dei casi si ha ontologicamente uno sfasamento temporale fra il momento in cui il profitto si realizza all'interno della realtà informatica e il momento in cui lo stesso assume materialità e fisicamente viene conseguito: ma ciò non significa che per aversi frode informatica sia necessario attendere questo secondo e ulteriore momento, che si sostanzia in post fatto non rilevante ai fini della tipicità, mera concretizzazione materiale di un vantaggio economico già totalmente e definitivamente acquisito.

La valutazione va condotta sulla base delle regole di funzionamento del singolo elaboratore elettronico o del singolo programma, in base alle quali un comando, un dato o un qualsiasi input assume immodificabilità all'interno dello stesso, diventando definitivamente di pertinenza di un soggetto.

2.8 L'elemento soggettivo

Sulla base delle disposizioni generali in tema di elemento soggettivo, si può dedurre che la frode informatica è una tipica fattispecie dolosa; l'art. 640-ter c.p. non prevede infatti la punibilità a titolo di colpa o preterintenzione, elementi psicologici eccezionali soggetti a riserva di legge in base alla regola sancita

all'art. 42 comma 2 c.p.[150].

Invero la stessa struttura della fattispecie presuppone un *quid* minimo di coscienza e volontà del fatto tipico, trattandosi di condotte volte precipuamente al conseguimento di un lucro, le quali implicano un certo dispendio di energie mentali, capacità tecniche e tempo d'azione: fattori che mal si conciliano con l'assenza di volontà e la violazione di regole cautelari tipiche della colpa.

Secondo l'opinione prevalente in dottrina e giurisprudenza, la frode informatica, al pari della truffa, richiede solamente il dolo generico, ossia la coscienza e volontà di realizzare tutti gli elementi costitutivi della fattispecie incriminatrice[151]: l'agente vuole e si rappresenta mentalmente ciò che realizza, almeno a livello di tentativo. In altri termini, fin dal momento in cui pone in essere la condotta di alterazione fraudolenta del funzionamento dell'elaboratore o di intervento indebito sui contenuti dello stesso, l'agente deve volere e rappresentarsi l'evento di danno, vale a dire l'irregolarità nel processo di elaborazione cui consegue il vantaggio patrimoniale e il danno altrui.

Vi sono poi alcuni – per la verità isolati – Autori di contrario avviso, i quali sostengono che per il delitto di frode informatica sia richiesto il dolo specifico, in quanto alla volontà-base di alterare il funzionamento di un elaboratore deve aggiungersi come intenzione ulteriore quella di "*procurare a sé od ad altri un ingiusto profitto con altrui danno*"[152].

Tale orientamento appare criticabile poiché in primis sconvolge la struttura normativa della fattispecie, nella quale l'elemento del profitto con danno altrui integra l'evento che deve conseguire causalmente alla condotta fraudolenta; non può arrestarsi allo stadio di elemento soggettivo particolare che deve caratterizzare la condotta dell'agente. Inoltre, non viene colta appieno la qualità

---

[150] L'art. 42 c. 2 c.p. dispone quanto segue: "*nessuno può essere punito per un fatto preveduto dalla legge come delitto, se non l'ha commesso con dolo, salvi i casi di delitto preterintenzionale o colposo espressamente preveduti dalla legge*"

[151] In tal senso, G. Pica, *op.cit*, F. Mucciarelli, "*Commento all'art. 10, L. 23 dicembre 1993, n. 547-Modificaizoni ed integrazioni alle norme del codice penale e di procedura penale in tema di criminalità informatica*", in Legislazione penale, 1996, pag. 139, G. Putzu in S. Logroscino, "*La frode informatica quale autonoma figura di reato rispetto al delitto di truffa*", articolo su Altalex del 21/12/2011; sul dolo generico, G. Fiandaca - E. Musco, "*Diritto penale, Parte generale*", Zanichelli, VI ed.

[152] D. D'Agostini, "*Diritto penale dell'informatica – Dai computer crimes alla digital forensic*", Esperta, Forlì, 2007, pag. 37; G. Faggioli, "*Computer crimes*", Simone, Napoli, 2002, pag. 149.

del dolo specifico, che consiste in uno scopo o in una finalità particolare ed ulteriore rispetto alla volontà di delinquere, che l'agente deve prendere di mira, ma che non è necessario si realizzi effettivamente perché il reato si configuri: anche prescindendo dal fatto che tale interpretazione non trova un riscontro testuale nella norma, si corre il rischio di rinvenire una frode informatica in qualsiasi alterazione di sistema effettuata con lo scopo di profitto e danno, la quale non arrivi però a causare materialmente un evento. In conclusione, si anticiperebbe notevolmente la soglia della punibilità, con il fondato pericolo di trasformare la fattispecie da reato di danno a reato di pericolo e di non riuscire più ad individuare una dimensione autonoma per il tentativo.

Nemmeno l'inciso "*senza diritto*" sembra presupporre un particolare fine che accompagni la condotta dell'agente: si tratta di una semplice clausola rafforzativa dell'antigiuridicità dell'intervento fraudolento sui contenuti informatici, inserita per richiamare sul punto l'attenzione dell'interprete. Ma, come visto, non richiede l'integrazione di un requisito ulteriore[153].

L'evento che caratterizza la fattispecie incriminatrice e che deve essere coperto dal dolo deve perciò essere "*preveduto e voluto dal soggetto agente come conseguenza della sua azione o omissione*" (art. 43 c. 1 c.p.): in altri termini, l'agente deve rappresentarsi mentalmente e volere tutti gli elementi caratterizzanti il fatto tipico, dalla condotta fraudolenta al profitto ingiusto con danno altrui. La dottrina pressoché unanime ritiene che sia il dolo intenzionale sia il dolo diretto possano integrare l'elemento soggettivo della frode informatica: la fattispecie delittuosa in esame è pacificamente compatibile con il grado massimo di rappresentazione e volontà dell'evento, in cui il fatto illecito costituisce l'obiettivo finalistico che dà causa alla condotta ed è altresì compatibile con quell'altro stato soggettivo in cui solo la rappresentazione dell'evento raggiunge l'intensità massima e la realizzazione del reato non è l'obiettivo principale dell'agente bensì costituisce soltanto strumento necessario per raggiungere uno scopo ulteriore[154]. Bisogna sottolineare come non sia necessario che l'agente si rappresenti come assolutamente certi entrambi gli

[153] Sul punto si rimanda al par. 4 cap. II.
[154] G. Fiandaca – E. Musco, *op.cit*.

eventi del reato (profitto e danno), essendo sufficiente che la previsione dell'evento avvenga nei termini di mera possibilità concreta; inoltre non è giocoforza richiesto il medesimo grado di volontà e rappresentazione criminosa per entrambi gli eventi, integrandosi una frode informatica anche nel caso in cui l'agente vuole e si rappresenta pienamente il proprio profitto e solamente accetta il rischio di danneggiare un terzo (e viceversa).

Per quanto concerne l'elemento implicito della causazione di un risultato irregolare del processo di elaborazione, anch'esso deve essere coperto da un coefficiente minimo di volontarietà: ciò non significa postulare il dolo intenzionale per tale requisito, poiché il preciso fine dell'agente di regola rimane il profitto per sé o per terzi con danno altrui, bensì significa richiedere per tale evento una consapevolezza minima, quale conseguenza della propria azione. L'agente deve aver ben presente che, nel momento in cui altera il funzionamento del sistema o interviene sui contenuti dello stesso per un vantaggio patrimoniale, causerà un malfunzionamento dello stesso rispetto alle istruzioni originariamente impartite, o per lo meno deve essere cosciente del rischio di causare tale anomalia pur non volendola: perciò tale evento intermedio deve essere coperto da dolo indiretto o per lo meno eventuale. Altrimenti il rischio è rinvenire una frode informatica nei casi di lesione al patrimonio altrui senza un ruolo di rilievo per l'ingerenza con il regolare svolgimento di un processo di elaborazione.

Ad ogni modo, si tratta di un requisito complesso da delineare, data la mancanza stessa dell'elemento in termini espressi e la poca attenzione in proposito mostrata dalla giurisprudenza: in questo senso, forse la scelta del legislatore di non richiederlo espressamente ha permesso ai giudici di evitare un problema applicativo piuttosto ostico, perché il dolo rimane pacificamente un elemento sempre difficile da provare.

Analizzando lo status soggettivo dal punto di vista della volontà criminosa, la fattispecie prevista dall'art. 640-ter c.p. appare compatibile, per la natura stessa del reato, tanto con il dolo di proposito quanto a maggior ragione con la

premeditazione[155]: la fenomenologia della fattispecie richiede che vi sia da parte dell'agente una seppur minima preparazione tecnica dell'intervento fraudolento, date le competenze specifiche richieste per operare su un sistema informatico o sui contenuti dello stesso, e conseguentemente che intercorra un certo lasso di tempo fra la fase dell'ideazione-progettazione e quella dell'esecuzione.

Anche l'elemento aggravante deve essere coperto da un minimo coefficiente soggettivo, al fine di poterlo contestare all'agente[156]. Ai fini dell'applicazione delle aggravanti di cui all'art. 640-ter c.p., è necessario verificare che sussista nell'un caso la precipua finalità dell'agente di causare un danno all'erario statale o ad un altro ente pubblico, nell'altro che vi sia la consapevolezza di agire in qualità di "*operatore del sistema*": tuttavia in entrambi le ipotesi non è necessario vi sia l'effettiva conoscenza dell'elemento circostanziale, bensì è sufficiente ex art. 59 c.p. che il reo abbia ignorato colposamente l'esistenza della circostanza aggravante[157]. La specifica colpevolezza relativa alle circostanze esige in tutti i casi un coefficiente minimo di imputazione ravvisabile nella "colpa": il reo deve essere nelle condizioni oggettive e soggettive di poter conoscere la previsione che aggrava la risposta sanzionatoria e ciononostante non esserne edotto a causa di un proprio comportamento negligente.

Un'attenzione particolare merita infine la nuova aggravante introdotta al terzo comma dell'art. 640-ter c.p., la quale richiede il "*furto o indebito utilizzo di identità digitale in danno di uno o più soggetti*": ancora non vi sono pronunce giurisprudenziali esplicative del nuovo elemento, ma è verosimile ritenere che il giudice dovrà verificare, ai fini della contestazione dell'aggravante anzidetta, che l'agente abbia la consapevolezza e la volontà sia di far uso della c.d. "identità digitale" senza titolo – o di essersene appropriato sempre sine causa – sia di arrecare in tal modo un danno altrui. Dalla formulazione normativa

[155] G. Putzu in S. Logroscino, "*La frode informatica quale autonoma figura di reato rispetto al delitto di truffa*", articolo su Altalex del 21/12/2011.

[156] Con la l. n. 13 del 7/02/1990, infatti, si è introdotto un regime di imputazione "soggettiva" anche per le circostanze aggravanti, alla luce del principio di responsabilità personale colpevole enunciato all'art. 27 Cost.

[157] L'art. 59 c. 1 c.p. che "*le circostanze che aggravano la pena sono valutate a carico dell'agente soltanto se da lui conosciute ovvero ignorate per colpa o ritenute inesistenti per errore determinato da colpa*".

sembra doversi desumere però che deve trattarsi di un'azione in danno ulteriore rispetto all'evento di danno richiesto dalla fattispecie base e del quale non è necessaria la piena verificazione. La formula "*in danno*" riferita all'azione fraudolenta la caratterizza in via soggettiva nell'atto in cui viene posta in essere: l'agente in altri termini deve rappresentarsi il danno che la sua condotta di furto o indebito utilizzo può causare, ma non è necessario ai fini della contestazione dell'aggravante che un danno ulteriore a quello di evento si realizzi concretamente[158].

Ad ogni modo, pur essendo un elemento descrittivo di tipo soggettivo, il dolo necessita di essere verificato alla stregua di parametri obiettivi, secondo massime di esperienza dalle quali sia possibile desumere che determinati comportamenti, atteggiamenti, e situazioni non possono non essere correlate alla volontà di causare l'evento lesivo.

[158] Nel capitolo III verranno analizzate le aggravanti.

Capitolo III: pena e circostanze aggravanti

3.1 Regime sanzionatorio; procedibilità; art. 640-ter comma 2 c.p.

Nella fattispecie di frode informatica è possibile individuare un'ipotesi base al comma primo, cui si aggiungono ai commi successivi delle ipotesi aggravate nelle quali cambia anche il regime della procedibilità. Il comma 1 infatti è caratterizzato dalla procedibilità a querela della persona offesa e da una sanzione cumulativa – pena detentiva e pena pecuniaria – forse non perfettamente adeguata in termini di effettività afflittiva: reclusione da 6 mesi a 3 anni e multa da euro 21,64 a euro 1.032,91.

La scelta di lasciare alla *voluntas persecutionis* della persona offesa la titolarità della repressione penale nel caso di specie, assieme ad una previsione sanzionatoria che, relativamente alla multa, risulta poco o nulla deterrente poiché non è stata proporzionata negli anni al costo della vita e alla crescita del volume di affari e delle occasioni per i criminali informatici, sono alcuni fra i fattori che hanno decretato la poca effettività della repressione sanzionatoria in ambito informatico: i *cyber crime* negli ultimi anni sono cresciuti vertiginosamente sia nel numero sia nelle dimensioni di attacco[1], ed è aumentata notevolmente anche la loro redditività. Perciò spesso il rischio di una sanzione che può arrivare a poco più di mille euro non scoraggia gli *hacker*, i quali sono consapevoli non solo di avere enormi margini di guadagno, ma anche e soprattutto di godere di molte probabilità di non essere scoperti, complici l'anonimato che spesso protegge chi opera su un sistema informatico o telematico e le difficoltà di cooperazione investigativa transfrontaliera. Forse sarebbe stato più opportuno prevedere un meccanismo di commisurazione

[1] Si parla di una variazione percentuale di più del 200% fra il 2011 e il 2014; per quanto riguarda la distribuzione degli attacchi nei vari settori, nel 2014 al primo posto assoluto rimane il settore governativo in senso esteso (inclusi anche gli enti a partecipazione pubblico-privata come INPS), con quasi un quarto degli attacchi. Al secondo posto, con un quinto degli attacchi, il gruppo "*Others*", a dimostrare quanto ormai gli attacchi gravi siano diffusi contro organizzazioni appartenenti ad ogni settore merceologico; cresce la gravità degli attacchi verso le categorie "*Online Services/Cloud*" (12% attacchi), "*Banking/Finance*" (6%), "*Health e Pharma*" (4%) e l'ampia categoria delle Associazioni (5%). La categoria "*Retail*" (che include la grande distribuzione organizzata, le catene di punti vendita in franchising ed i siti di e-commerce) entra prepotentemente nel mirino dei cyber criminali, registrando globalmente perdite ingentissime rispetto al numero di attacchi di cui si ha notizia; vedi rapporto Clusit per il 2015.

della sanzione che facesse riferimento al profitto conseguito dall'agente[2], piuttosto che una sanzione pecuniaria avulsa dal contesto nel quale si svolge l'offesa.

La poca effettività della sanzione deriva anche dal tipo scelto: moltissimi Autori oggi sottolineano l'inutilità della sanzione privativa della libertà personale soprattutto in relazione alle lesioni patrimoniali, poiché non rieducativa e spesso anzi criminogena. Nello specifico caso dello frode informatica, la fenomenologia della fattispecie insegna come spesso ci sia ben poco da "rieducare" nei *computer criminals*: in molti casi si tratta di soggetti giovani, ben istruiti, competenti e pienamente integrati nel proprio contesto sociale, i quali desiderano testare le proprie capacità o procacciarsi una fonte di guadagno ulteriore di cui non percepiscono la contrarietà all'ordinamento. Perciò in questo caso più che in altri è necessario che lo Stato e gli enti pubblici, in collaborazione con il settore privato, intervengano in via preventiva, individuando da una parte metodi e strumenti per rafforzare la consapevolezza dell'offensività e dell'illiceità degli abusi informatici e dall'altra studiando barriere e misure di sicurezza efficaci, tali da bloccare e individuare la condotta criminale prima che causi l'evento di danno[3].

Anche la perseguibilità a querela gioca un ruolo importante: blocca all'origine la risposta dell'ordinamento e quindi la punibilità di molti casi in cui nondimeno la gravità del danno o le circostanze del caso concreto esigerebbero una risposta effettiva e deterrente in termini generalpreventivi. Perciò anche la richiesta di querela contribuisce indirettamente ad acuire la difficoltà di percepire la frode informatica come contraria all'ordinamento. Nella maggior parte dei casi infatti, le imprese preferiscono non denunciare gli accessi abusivi al proprio sistema informatico o le frodi, poiché ciò potrebbe irrimediabilmente danneggiare la loro credibilità ed affidabilità di fronte al pubblico dei clienti, causando perdite di gran

[2] Un criterio di questo tipo sta alla base delle sanzioni pecuniarie "per quote" che colpiscono gli enti i quali si trovano a dover rispondere per un illecito penale. Il d.lgs. n. 231/2001 infatti ha introdotto un meccanismo per cui la sanzione pecuniaria consiste in quote, il numero delle quali viene individuato in base alla gravità del fatto e al grado di responsabilità dell'ente; in seconda battuta l'organo giurisdizionale determina il valore monetario della singola quota, sulla base delle condizioni economiche e patrimoniali della persona giuridica. Simile è anche il sistema sanzionatorio di quantificazione della *multa per dias* in vigore in Spagna: cap. VII.

[3] Al cap. VI vengono analizzate le iniziative di tipo preventivo in Italia e a livello europeo ed internazionale.

lunga superiori a quelle determinate dal delitto in sé considerato.

L'intervento repressivo da parte dello Stato opera d'ufficio nel momento in cui è possibile contestare una circostanza aggravante, sia essa richiamata dallo stesso art. 640-ter c.p. oppure collocata altrove (art. 640-ter c. 4 c.p.); il secondo comma fa dapprima rinvio alle circostanze aggravanti in tema di truffa previste al secondo comma n. 1 dell'art. 640 c.p., poi aggiunge una specifica circostanza aggravante riferita alla commissione del reato in qualità di "operatore di sistema": in tali casi "*la pena è della reclusione da uno a cinque anni e della multa da trecentonove euro a millecinquecentoquarantanove euro"*. Essendo stato abolito l'obbligo del servizio militare (e comunque essendo difficile immaginare una frode informatica commessa a tal fine; l'indagine criminologica testimonia la poca accuratezza del rinvio legislativo, poiché si tratta di solito di autori teleologicamente orientati a finalità economiche-lucrative), oggi il richiamo al n. 1 del c. 2 art. 640 c.p. può ritenersi esclusivamente rivolto al caso di frode informatica commessa in danno dello Stato o di un altro ente pubblico[4].

In questo caso la sanzione è rafforzata anche dalla previsione della responsabilità da reato per la persona giuridica che si avvantaggia della commissione della frode informatica o non ha posto in essere i c.d. modelli organizzativi idonei per evitare la commissione di reati: l'art. 24-bis del d.lgs. n. 231/2001 prevede una sanzione pecuniaria che può arrivare fino a 500 quote nell'ipotesi-base e da 200 a 600 quote nel caso di ipotesi aggravata da un profitto di rilevante entità. In tale ultimo caso inoltre è prevista l'applicazione ex lege di sanzioni interdittive, che possono risultare molto gravose per l'ente: si tratta del divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio; l'esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli già concessi; il divieto di pubblicizzare beni o servizi[5].

[4] Stupisce il mancato riferimento all'Unione Europea: seppur con qualche forzatura può essere inclusa nell'ambito applicativo dell'aggravante in esame come "ente pubblico".

[5] L'art. 24 d.lgs. n. 231/2001 "Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico" dispone quanto segue: *1. In relazione alla commissione dei delitti di cui agli articoli 316-bis, 316-ter, 640, comma 2, n. 1, 640-bis e 640-ter se commesso in*

L’ammontare della sanzione in quote, commisurato anche alla condizione economica dell’ente, assieme al forte impatto e alle conseguente dissuasività delle sanzioni interdittive conferiscono alla sanzione che colpisce la persona giuridica una notevole dose di effettività.

Il comma 2 dell’art. 640-ter c.p. prevede anche una circostanza aggravante speciale, riferita al caso di truffa commessa con abuso della qualità di operatore di sistema. La *ratio* di quest’ultima disposizione appare evidente: la condotta fraudolenta posta in essere da un soggetto che viola un dovere di fedeltà nei confronti del titolare del sistema informatico e delle persone i cui interessi economici sono gestiti dallo stesso appare particolarmente grave, a maggior ragione per le possibilità materiali di intervenire abusivamente sui contenuti informatici, cui corrisponde una situazione di accentuata vulnerabilità dei dati, delle informazioni e dei programmi stessi.

Si tratta di una aggravante ad effetto speciale di tipo soggettivo, incentrata tutta sul significato da attribuire alla nozione di “*operatore di sistema*”.

Cercando di definire il concetto prima in negativo, sicuramente non si potrà ritenere “operatore di sistema” qualsiasi soggetto in grado di interagire con un sistema informatico, il quale sia venuto a contatto con lo stesso in via occasionale (come ad es. un tecnico informatico o un programmatore): costui non disporrà delle conoscenze specifiche del sistema bensì sarà in grado solo di svolgere quelle limitate operazioni (di programmazione, pulizia e controllo) “standard” per ogni sistema del tipo di quello in questione (per es. una formattazione di sistema operativo). L’applicazione dell’aggravante presuppone che vi sia un particolare legame fra l’agente e il sistema informatico: perciò non è sufficiente avere una generale competenza in ambito informatico per poterla applicare.

Per quanto riguarda il semplice operatore di *consolle*, bisogna distinguere a seconda della confidenzialità della sua posizione rispetto ai dati contenuti nel

---

danno dello Stato o di altro ente pubblico, del codice penale, si applica all'ente la sanzione pecuniaria fino a cinquecento quote. 2. Se, in seguito alla commissione dei delitti di cui al comma 1, l'ente ha conseguito un profitto di rilevante entità o è derivato un danno di particolare gravità, si applica la sanzione pecuniaria da duecento a seicento quote. 3. Nei casi previsti dai commi precedenti, si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e).

sistema informatico: è vero che si tratta di un soggetto che si limita a svolgere funzioni meramente esecutive e manuali, ma è anche vero che potrebbe godere di un particolare accesso a dati sensibili che sarebbero così più esposti a rischi o comunque potrebbe avere più opportunità, attraverso questo suo ruolo, di frodare ignare vittime. Mucciarelli per questo considera operatore di sistema anche colui il quale riveste una particolare qualifica professionale o possiede conoscenze ulteriori e specifiche rispetto a quelle di ogni "operatore di sistema" inteso come mero esecutore di operazioni quasi meccaniche.

Proseguendo verso il fulcro della nozione, dovrà positivamente ritenersi operatore di sistema solo un particolare tecnico specializzato, quello che ha il controllo o la disponibilità delle varie fasi del processo di elaborazione di dati all'interno di un azienda o di un *database* e quindi ha la facoltà, conferita *ex lege* o *ex contractu*, di inserirsi in tutti i settori della memoria interna del sistema, attraverso un canale di accesso riservato e privilegiato. In altri termini si tratta sia del c.d. *system administrator*[6] sia delle specializzazioni in *database administrator* e *network administrator*, equiparabili al primo dal punto di vista della responsabilità ricoperta e della sicurezza dei dati trattati. Costoro devono gestire a livello infrastrutturale nel primo caso il buon governo dell'hardware e/o del software (sia lato client sia lato server) del sistema, nel secondo specificamente una base di dati e nell'ultimo una rete di calcolatori e relativi apparati di networking, affinché funzionino in modo corretto ovvero affinché l'insieme dei servizi offerti possa essere erogato nella maniera più efficiente possibile agli utenti, divenendone dunque responsabile.

Dal punto di vista giuridico perciò la nozione di amministratore di sistema viene notevolmente ampliata rispetto alla corrispondente nozione in ambito informatico, per essere caratterizzata in via teleologica ed inglobare tutti coloro che si trovano in una posizione di particolare responsabilità rispetto ad un sistema informatico o ai contenuti dello stesso: a riprova di questo

[6] Nel *Dizionario dei termini di Informatica* viene definito "amministratore di sistema" colui che è responsabile della gestione di un sistema informatico multiutente, di un sistema di comunicazione o di entrambi; tra le funzioni svolte dagli amministratori di sistema vengono indicate la "assegnazione agli utenti degli account e delle password, la definizione di livelli di accesso sicuri e l'allocazione dello spazio di memorizzazione", nonché quella di "controllare che non si verifichino accessi non autorizzati e di impedire che virus e cavalli di Troia entrino nel sistema".

orientamento, il Garante per la protezione dei dati personali propone una definizione che si discosta da quella tecnica, considerando "amministratore di sistema" sia quelle figure professionali che "*si individuano generalmente, in ambito informatico*, (in quanto) *finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti*. […] *vengono però considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi. Gli amministratori di sistema così ampiamente individuati, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio applicativo (significato dei dati, formato delle rappresentazioni e semantica delle funzioni)*, *nelle loro consuete attività sono, in molti casi, concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati*."[7]

Lo stesso Garante sottolinea come sostanzialmente il legislatore si sia riferito a tali soggetti nell'individuare particolari funzioni tecniche come circostanze aggravanti, se svolte da chi commette un determinato reato: fra queste richiama proprio la qualità di operatore di sistema dell'art. 640-ter comma 2 c.p..

Oltre a determinare un aumento dei limiti edittali della pena, la circostanza che la condotta integri gli estremi dell'aggravante prevista al comma 2 art. 640-ter prima parte comporta altresì l'applicabilità del disposto dell'art. 640-quater c.p., che prevede per questi casi l'applicabilità, in quanto compatibile, dell'art. 322-ter c.p.[8]

Attraverso questo rinvio – che peraltro fa salvo discutibilmente il caso di frode informatica commessa da un operatore di sistema – è fatto obbligo al giudice di

[7] Provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 recante "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alla attribuzione delle funzioni di amministratore di sistema*", pubblicato sulla G.U. n. 300 del 24/12/2008: "*con il presente provvedimento il Garante intende richiamare tutti i titolari di trattamenti effettuati, anche in parte, mediante strumenti elettronici alla necessità di prestare massima attenzione ai rischi e alle criticità implicite nell'affidamento degli incarichi di amministratore di sistema*".

[8] L'art. 640-quater c.p. così dispone: *"nei casi di cui agli articoli 640, secondo comma, numero 1, 640bis e 640-ter, secondo comma, con esclusione dell'ipotesi in cui il fatto è commesso con abuso della qualità di operatore del sistema, si osservano, in quanto applicabili, le disposizioni contenute nell'articolo 322ter".*

ordinare sempre la confisca dei beni che costituiscono il profitto o il prezzo del reato, salvo che appartengano a persona estranea al reato: pertanto viene in considerazione qualsiasi utilità economicamente valutabile (patrimoniale e non), direttamente derivante dalla commissione del fatto illecito, sia essa frutto del reato ovvero beni o vantaggi dati o promessi al reo affinché delinqua. Tali beni verranno sempre sottratti alla disponibilità del reo con la sentenza di condanna o di applicazione della pena su richiesta delle parti, a prescindere da qualsiasi valutazione discrezionale dell'organo giudicante.

Allorquando non sia possibile la confisca specificamente dei beni che sono frutto dell'attività illecita o costituiscono il corrispettivo per l'esecuzione della stessa, l'art. 322-ter c.p. prevede l'istituto della confisca per equivalente, ovvero "*dei beni, di cui il reo ha la disponibilità, per un valore corrispondente a tale prezzo o profitto*".

Fin dall'introduzione nel 2000 dell'art. 640-quater c.p., si è posto il problema dell'applicabilità di tale istituto alle fattispecie di truffa, poiché il rinvio è operato in generale alle previsioni dell'art. 322-ter c.p. ma solo "*in quanto compatibili*" e la confisca per equivalente era prevista specificamente con riguardo alla fattispecie di cui all'art. 321 c.p. ("corruzione attiva"). Con la modifica normativa del 2012, che ha aggiunto espressamente al c. 1 la confisca per equivalente anche del profitto del reato, è stato risolto un serio problema applicativo che negli anni aveva creato un vivace dibattito in dottrina e giurisprudenza: l'orientamento maggioritario e più restrittivo riteneva che il rinvio operato dall'art. 640-quater c.p. si riferisse solo alle disposizioni generali di cui al comma primo dell'art. 322-ter c.p., dove si prevedeva la confisca del profitto del reato e l'azione per equivalente solo nei confronti del prezzo dello stesso; perciò non poteva aversi confisca per equivalente del profitto del reato, a meno di non voler sfociare in un'applicazione analogica *in malam partem* del dettato normativa. Altro orientamento, avvalorato nel 2005 anche da una pronuncia della Sezioni Unite, prendendo le mosse dalla generalità del rinvio operato dall'art. 640-quater c.p., proponeva di applicare la confisca per equivalente ai reati di truffa attraverso il comma 2 dello stesso art. 322-ter c.p., nel quale però essa era stata prevista esclusivamente "*per il delitto previsto dall'articolo 321*".

Tale opinione fu presto accolta in alcune pronunce di singole sezioni di Cassazione, nelle quali i giudici hanno sottolineato come escludere la confisca per equivalente del profitto nei reati di truffa fosse contrario alla *ratio* ispiratrice dell'art. 640-quater, introdotto nel 2000 al fine di contrastare in maniera più diretta ed efficace l'indebita percezione di fondi, finanziamenti o sussidi pubblici[9]. La Corte di Cassazione ha affermato che ai sensi dell'art. 640-*quater* c.p. tale misura è ammessa a carico del responsabile del reato, ancorché il profitto sia stato conseguito da un terzo estraneo al fatto, persino non indagato. La Corte giunge dunque a ritenere legittima la confisca di beni di cui l'agente ha effettiva disponibilità fino a concorrenza di un valore corrispondente al profitto, proprio, di concorrenti o di terzi, conseguito mediante le condotte fraudolente[10].
Con la sent. n. 41936 del 2005 anche le Sezioni Unite hanno confermato la legittimità di questa ricostruzione, sottolineando come dal punto di vista formale *"la lettera dell'art. 640-quater opera un rinvio indifferenziato alle disposizioni contenute nell'art. 322-ter c.p.",* senza porre distinzioni tra il primo ed il secondo comma: perciò era pienamente legittima l'interpretazione dell'art. 640-quater c.p. nel senso di ritenere applicabile la confisca per equivalente al profitto delle truffe aggravate ai danni dello Stato. Anzi, autorevole dottrina rileva come si tratti dell'unica soluzione ragionevole, dato che per i reati di truffa richiamati dall'art. 640-quater c.p. non è ipotizzabile la nozione di "prezzo" del reato[11].
Con la novella del 2012 il legislatore ha scelto di positivizzare l'interpretazione giurisprudenziale più sostanzialistica e attenta all'effettività della risposta penale, conferendole chiarezza e indubitabilità.

[9] Cass. Pen., sez. I, sent. n. 9395 del 9/03/2005,; Cass. Pen., sez. II, sent. n. 31990 del 14/06/2006, nella quale si stabiliva la legittimità del sequestro per equivalente, pur mediato da una valutazione attenta caso per caso; Cass. Pen., sez. VI, sent. n. 37090 del 30/05/2007.
[10] Cass. Pen., sez. VI, sent. n. 16669 del 11/03/2009, *Pubblico Ministero presso Tribunale di Palermo c. S.C.*, nella quale era stato ritenuto legittimo il sequestro preventivo per equivalente di beni appartenenti ad un commercialista che, in concorso con funzionari dell'Agenzia delle Entrate, aveva ottenuto, intervenendo abusivamente nel sistema informatico dell'anagrafe tributaria, uno sgravio fiscale in favore dei suoi clienti.
[11] G. Amato, nota a sent. Sez. Unite n. 41936 del 25/10/2005, *Muci*, "Guida dir.", 2005, n. 47, 52.

3.2 Art. 640-ter comma 3 c.p.: frode informatica commessa con "*furto o indebito utilizzo di identità digitale*"

Nel 2013, al fine di fronteggiare in maniera effettiva le condotte di sottrazione di dati sensibili sulla rete Internet per conseguire un illecito profitto o per danneggiare ignari utenti, il Governo ha introdotto nell'art. 640-ter c.p. una nuova statuizione normativa attraverso l'emanazione del decreto-legge n. 93 recante "*Disposizioni urgenti in materia di sicurezza per il contrasto della violenza di genere, nonché in tema di protezione civile e di commissariamento delle province*"; si trattava di un provvedimento "*omnibus*", volto ad arginare molteplici fenomeni che destavano e destano forte allarme sociale[12].

L'art. 9 comma 1, lett. a) della legge di conversione 15 ottobre 2013, n. 119 ha così introdotto il comma 3 all'art. 640-ter c.p., disponendo che "*la pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti*".

Con tale previsione il Parlamento ha radicalmente mutato quanto era stato precedentemente stabilito nel decreto legge, ove si prevedeva la medesima sanzione bensì per il caso in cui il fatto venisse commesso "con sostituzione di identità digitale in danno di uno o più soggetti"; veniva introdotta quindi una nuova locuzione –"furto o indebito utilizzo" – che ha sollevato un vivace dibattito in merito al significato, alla portata applicativa e ai limiti, a causa delle varie questioni lasciate irrisolte dallo stesso legislatore.

Il primo aspetto che ha fatto discutere in dottrina è la natura del *novum* legislativo: se è vero infatti che vi sono ragioni – come la collocazione sistematica e il tenore letterale – che lo fanno intendere come circostanza aggravante speciale, è pur vero che potrebbe essere considerato una fattispecie autonoma, posta a tutela di un bene giuridico diverso rispetto al patrimonio, ossia la tutela della riservatezza in ambito informatico e

[12] In questo decreto "omnibus" il Governo è intervenuto sulla disciplina delle fattispecie di maltrattamenti in famiglia, atti persecutori e violenza sessuale, sia agendo sulla cornice edittale sia prevedendo nuove circostanze aggravanti e nuove misure pre-cautelari; vengono poi introdotte nuove aggravanti dei reati di furto, rapina, ricettazione a tutela di attività di particolare rilievo strategico nonché per garantire soggetti deboli come anziani e minori. Vedi Rel. Cass. n. III/01/2013, Roma, 22/08/2013.

dell'affidabilità dei sistemi informatici e telematici come veri e propri luoghi ove utilizzare senza rischi i propri dati sensibili e crearsi quindi un'identità.

A ben vedere, sia ragioni di tipo formale sia ragioni di tipo sostanziale fanno propendere per la natura di circostanza aggravante dell'integrazione legislativa: infatti, alla luce di quanto previsto all'ultimo comma dell'art. 640-ter c.p., ove si definisce la procedibilità stabilendo che "*il delitto è punibile a querela della persona offesa salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o un'altra circostanza aggravante*", appare evidente come la scelta del legislatore sia stata proprio quella di introdurre una vera e propria circostanza aggravante che implicasse una sanzione maggiorata per la particolare modalità di verificazione della frode informatica così come prevista dal comma 3 in rapporto al comma 1[13].

Pertanto, in base al principio *genus–species* che lega l'ipotesi generale a quelle aggravate, bisogna concludere che attraverso il comma 3 dell'art. 640-ter c.p. si sia voluto positivizzare una specificazione della condotta tipica di cui al c. 1[14].

La novella considera esplicitamente due modalità d'azione, quella di "*furto*" e quella di "*indebito utilizzo*", le quali hanno come oggetto immediato la c.d. identità digitale: soprattutto la seconda condotta, negli anni precedenti, è stata oggetto di vivaci discussioni poiché non tutti gli Autori concordavano sulla possibilità di includerla nella fattispecie di frode informatica. Infatti, nel nostro art. 640-ter c.p. non vi è un riferimento esplicito alla condotta di uso indebito di dati, ma è contemplato unicamente l'"*intervento senza diritto su dati, informazioni o programmi*", nel senso di modificazione del contenuto o della destinazione degli stessi. In precedenza si è cercato di spiegare come autorevole dottrina abbia cercato di includere tale condotta nel delitto in esame spostando l'attenzione dell'interprete dal momento di utilizzo indebito dei dati a quello nel quale avviene lo spostamento patrimoniale – e quindi l'arricchimento indebito con altrui danno – successivo all'introduzione nel profilo altrui[15], lasciando al presidio di altre fattispecie la sanzione del mero accesso effettuato

[13] "*La frode informatica commessa con sostituzione d'identità digitale: profili applicativi*", di Antonio di Tullio D'Elisiis del 14/01/2014, reperibile su Altalex.
[14] T. Padovani, "*Diritto Penale*", X ed., Milano, 2012.
[15] Riferimento al par. 4 cap. II, pag. 4, C. Pecorella, *op.cit.*

in maniera abusiva. Sulla base di tale impostazione, è possibile corroborare la collocazione sistematica e la natura del comma 3 come circostanza aggravante integrata nell'art. 640-ter c.p. al precipuo fine di sanzionare con più incisività quelle condotte già sanzionabili ex art. 640-ter c. 1 c.p. nel momento in cui avviene lo spostamento patrimoniale, ma ritenute maggiormente offensive proprio alla luce della particolare modalità dell'intervento sui dati stessi, che implica una sostituzione d'identità in senso lato.

Si tratta comunque di un aspetto problematico, poiché non tutti gli Autori considerano integrato il delitto di frode informatica nel caso di mero uso indebito di dati: con la conseguenza che tale condotta, espressamente inclusa nell'art. 640-ter c.p. solamente nel 2013, troverebbe un presidio penale per la prima volta grazie a questa integrazione, da considerarsi quindi una nuova fattispecie incriminatrice.

Ragionando in termini di bene giuridico tutelato, difficilmente si può considerare il *novum* legislativo una nuova previsione incriminatrice, poiché il bene tutelato rimane sempre *in primis* il patrimonio: il fatto è costituito pur sempre da una frode informatica ritenuta più grave proprio in virtù delle lesioni (strumentali) alla riservatezza informatica e alla sicurezza ed affidabilità nell'uso della propria identità in ambito virtuale[16]. Si tratta di una lesione strumentale rispetto alla realizzazione della condotta offensiva, che rimane quella descritta dal c. 1 dell'art. 640-ter c.p. ma che la rende più offensiva e quindi meritevole sia di una sanzione più incisiva sia della perseguibilità d'ufficio[17].

Nello specifico il comma 3 art. 640-ter costituisce una circostanza speciale, poiché riguardante il solo delitto di frode informatica, ad effetto speciale, stante la previsione di una diversa cornice edittale superiore ad un terzo.

Il furto d'identità in sé considerato è stato ricondotto dalla giurisprudenza di legittimità, in mancanza di una fattispecie incriminatrice specifica, nell'ambito

[16] Nella disposizione infatti si legge "*se il fatto* (di cui al c. 1) *è commesso con*".

[17] In effetti, la novella si esprime con un generico "*se il fatto è commesso con*" e non con un "*se il fatto consiste in*", pertanto specifica soltanto delle modalità che possono portare alla perfezione del fatto tipico: articolo di G. Malgieri, "*La nuova fattispecie di indebito utilizzo d'identità digitale, un problema interpretativo*", del 22/10/2014, reperibile su www.penalecontemporaneo.it.

del delitto previsto all'art. 494 c.p. che sanziona la "sostituzione di persona"[18].
La Corte di Cassazione ha rilevato la lesione della pubblica fede e la conseguente integrazione del delitto sopra citato nel comportamento di colui che crei ed utilizzi un account di posta elettronica o un profilo su social network, attribuendosi falsamente le generalità di un diverso soggetto e inducendo in errore gli altri utenti della rete Internet con il fine di arrecare danno al soggetto cui le generalità erano state in precedenza sottratte[19].
Sorvolando sul delicato problema della delineazione del concetto di pubblica fede, relativamente all'offensività della condotta emerge dai giudici di legittimità un chiaro orientamento: le condotte cui il legislatore con il comma 3 dell'art. 640-ter vuole dare rilevanza penale nell'ambito della frode informatica avevano già trovato presidio penale, nel caso si trattasse di "furto", attraverso l'applicazione estensiva dell'art. 494 c.p. che, in quanto reato di pericolo, anticipa la soglia della punibilità, consumandosi già nel momento in cui l'agente spende una identità non propria avendo meramente il fine di avvantaggiarsi o di arrecare un danno. La disposizione di cui al comma 3, quindi, ha introdotto un'importante novità andando a regolamentare il furto d'identità (nella nuova accezione di *identità digitale*) come modalità d'azione per commettere una frode informatica, colmando una lacuna legislativa che con l'avvento di Internet e in special modo del web 2.0 negli ultimi anni si è particolarmente avvertita: in molti casi infatti può risultare davvero forzato ed anacronistico far rientrare determinate tipologie di reato, tipiche della nuova era tecnologica, nell'ambito del Capo IV del Titolo VII del Codice penale, "*Dei delitti contro la fede pubblica – falsità personali*"[20].

[18] Art. 494 c.p.: "*Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici, è punito, se il fatto non costituisce un altro delitto contro la fede pubblica, con la reclusione fino a un anno".*
[19] Cass. Pen., sez. V, sent. n. 46674 del 8/11/2007; Cass. Pen., sez. V, sent. n. 25774 del 16/06/2014.
[20] Come nel caso risolto con la sent. 25774 del 16/06/2014, nel quale l'imputato creò un profilo sul social network "*Badoo*" sfruttando l'immagine della persona offesa, con una descrizione dettagliata e poco lusinghiera (informazioni personali di carattere dispregiativo); attraverso tale falsa identità usufruiva dei servizi del sito, consistenti essenzialmente nella possibilità di comunicazione in rete con gli altri iscritti (indotti in errore sulla sua identità) e di condivisione di contenuti. In tal caso vi sarebbero forse stati gli estremi per contestare la frode informatica

L'introduzione del comma 3 ha conferito risalto alla forte carica offensiva che il furto o l'indebito utilizzo di identità digitale possiedono nel momento di perpetrazione di una frode informatica, ampliando in parte il fatto tipico previsto dall'art. 494 c.p. e dalla prima versione della circostanza nel decreto-legge attraverso la locuzione "*furto o indebito utilizzo*" di identità digitale, al posto della sua "*sostituzione*". In questo modo l'aggravante in esame opera sia nel caso vi sia un vero e proprio furto, sempre presupponendo che possa sussistere un furto di un'entità immateriale come un'identità, sia nel caso di semplice indebito utilizzo, ovvero quella situazione nella quale non è possibile rinvenire propriamente una sottrazione di *res* altrui, ma l'offensività della condotta si concentra nell'uso senza facoltà legittima di dati di terzi da parte di un soggetto che ne ha la legittima disponibilità.

L'altro merito della novella del 2013 è quello di rendere più agevoli l'indagine e la successiva contestazione da parte degli organi inquirente e giudicante, dato che il fatto tipico rimane solo uno ancorché aggravato: l'autorità giudiziaria deve limitarsi ad individuare gli elementi costitutivi di un unico reato, la frode informatica, valutando nel contempo se la modalità commissiva della stessa integri altresì gli estremi della aggravante in commento. Si tratta di un lavoro diverso e meno oneroso rispetto alla necessità di riscontrare nel caso concreto tutti gli elementi del furto di identità ex art. 494 c.p. sì da poterlo contestare in concorso con la frode informatica: in questo caso infatti vi sarebbero degli elementi costitutivi ulteriori da sempre complessi da dimostrare come il dolo specifico, l'induzione in errore derivante causalmente dalla condotta criminosa e la lesione alla fede pubblica.

Una delle prime questioni spinose è stata definire il concetto di identità digitale, visto che il legislatore non ha affatto fornito una definizione in proposito, pur venendo rimarcata in sede di lavori parlamentari l'opportunità di una norma giuridica di questo genere: in assenza di una definizione, si rilevava il pericolo di

aggravata dal furto di identità digitale. Articolo "*Web 2.0: la Cassazione interviene su un caso di sostituzione di persona*", Cass. Pen., sez. IV, sentenza n. 25774 del 16/06/2014, di Michele Iaselli, reperibile su Altalex.

un interpretazione eccessivamente lata o che creasse disparità di trattamento[21].
Fin dai primi interventi di autorevole dottrina, si è tentato di individuare dei confini più definiti per la nozione di identità digitale, andando a recuperare una possibile definizione in sede extra-penale dall'art. 1 c. 1 lett. u-ter) del D.lgs n. 82 del 7/05/2005, c.d. "Codice dell'Amministrazione digitale". Qui si rinviene una definizione di "*identificazione informatica*", quale "*validazione dell'insieme di dati, attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso*".
Tuttavia sono d'obbligo due rilievi: in primis, guardando al dato formale si può rilevare come le definizioni fornite dal codice dell'Amministrazione Digitale siano fornite espressamente "*ai fini del codice*" stesso (art. 1) e la portata applicativa del testo normativo individua come destinatari solo lo Stato, le regioni e le province autonome, ed è circoscritta al mero fine di assicurare "*la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale*" (art. 2 c. 1).
Inoltre, a conferma della difficoltà di sfruttare questa norma come valido riferimento ermeneutico, soccorre anche il fatto che durante i lavori parlamentari fu presentato un emendamento, volto a sostituire la locuzione "*identità digitale*" con "*identità ai fini dell'identificazione informatica in danno ad uno o più soggetti*"[22]: tale circostanza testimonia come la locuzione "identificazione informatica" non sia stata da tutti ritenuta eguale o corrispondente all'espressione "identità digitale" e che vi erano sensibilità differenti fra i componenti dell'Aula, alcune delle quali maggiormente attente all'aspetto tecnico relativo alla scelta di una locuzione piuttosto di un'altra.
Cionondimeno, la scelta successiva fu quella di ritirare l'emendamento, poiché "*la giurisprudenza della Cassazione contiene già, nell'identità informatica, il*

[21] Interventi On. P. Coppola e S. Boccadutri innanzi alla Camera dei Deputati, seduta n. 93 del 9/10/2013, in www.camera.it.
[22] Emendamento *Quintarelli* pubblicato nell'allegato A degli atti della seduta dell'Aula del 9/10/2013, Camera dei Deputati, ma vedi anche gli interventi in aula degli onorevoli Coppola, Schirò Planeta, Palmieri, Boccadutri, De Lorenzis, resoconto stenografico dell'Assemblea, seduta n. 93 di mercoledì 9 ottobre 2013, Camera dei Deputati, XVII Legislatura.

concetto di identità digitale"[23]: non pare l'opzione migliore, dato che la Cassazione non è tenuta a creare norme valide *erga omnes* ed essendo necessario per l'operatore del diritto un canone di tipo legislativo rispetto al quale misurare la propria interpretazione, anche al fine di evitare risultati non equi o discriminatori.

Nel tentativo di delineare i confini all'identità digitale, un importante contributo fu quello esposto da Caterina Flick[24], poi condiviso anche dalla Corte di Cassazione[25]. I giudici di legittimità, dopo aver ribadito la natura di circostanza aggravante del *novum* legislativo, hanno definito l'identità digitale utilizzando le parole della Flick come "*l'insieme delle informazioni e delle risorse concesse da un sistema informatico ad un particolare utilizzatore del suddetto sotto un processo di identificazione che consiste* – e qui viene ripreso il contenuto dell'art. 1 lett. u-ter) del D.lgs. 7 marzo 2005, n. 82 – *nella validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso*". Facendo ricorso al linguaggio comune, è possibile conferire un'accezione ancora più lata al concetto in esame, comprendendovi l'"insieme di informazioni presenti on-line e relative ad un soggetto/ente/brand/ecc"[26].

Successivamente nel 2014, il percorso normativo dell'identità digitale è andato specificandosi, essendo stata introdotta nel sistema una definizione alquanto ristretta, ai soli fini della creazione e sviluppo del Sistema Pubblico per la gestione delle Identità Digitali di cittadini ed imprese[27]: nel decreto della Presidenza del Consiglio dei Ministri, l'art. 1 c. 1 lett. o) definisce l'identità digitale come la "*rappresentazione informatica della corrispondenza biunivoca*

---

[23] Intervento On. A. Gargano tenutasi innanzi alla Camera dei Deputati, seduta n. 93 del 9/10/2013, in www.camera.it.

[24] Caterina Flick, "*Falsa identità su internet e tutela penale della fede pubblica degli utenti e della persona*", in Rivista di Diritto dell'Informazione e dell'Informatica, 2008, 4-5, 526.

[25] Rel. n. III/01/2013, Roma 22/08/2013, "*Novità legislative: D.L. 14 agosto 2013, n. 93 «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»".*

[26] Definizione di Wikipedia reperibile al link: it.wikipedia.org/wiki/Identità_digitale.

[27] Decreto della Presidenza del Consiglio dei Ministri 24 ottobre 2014, pubblicato sulla Gazzetta Ufficiale n. 285 del 9 dicembre 2014, intitolato "*Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale, nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese*".

tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità di cui al presente decreto e dei suoi regolamenti attuativi"[28]. Anche in questo caso però sembrerebbe rimandarsi più ad una metodologia che consente l'identificazione informatica, piuttosto che ad un vero e proprio concetto di identità digitale.

Un altro intervento ancor più recente in materia di identità digitale sono le disposizioni contenute nel Regolamento UE n. 910/2014 relative alla procedura di identificazione elettronica e ai servizi fiduciari per le transazioni elettroniche nel mercato interno[29] che saranno operative a partire dal 1° luglio 2016: il provvedimento, direttamente applicabile in tutti gli Stati membri, stabilisce una serie di condizioni per il riconoscimento reciproco dei sistemi di autenticazione elettronica, regole comuni per le firme elettroniche e per l'autenticazione web. All'art. 3 il Reg. eIDAS introduce una serie di definizioni preliminari, riferendosi però non al concetto di identità digitale, bensì distinguendo quello – più corretto – di "*identificazione elettronica*", rispetto ai "*dati di identificazione personale*", nozione forse più precisa per indicare un'identità intesa come insieme di dati.

L'"identificazione elettronica" è quel "*processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentano un'unica persona fisica o giuridica, o un'unica persona fisica che rappresenta una persona giuridica*"; i dati risultano utili per costituire un "regime di identificazione elettronica", cioè un sistema nel quale si forniscono mezzi per identificare in via univoca un soggetto all'interno di un sistema, procedendo alla vera e propria "autenticazione". I "dati di identificazione personale" costituiscono invece un

[28] Il sistema SPID è costituito come insieme aperto di soggetti pubblici e privati (cittadini e imprese) che, previo accreditamento da parte dell'Agenzia per l'Italia Digitale, gestiscono i servizi di autenticazione, ovvero registrazione e messa a disposizione delle credenziali e degli strumenti di accesso in rete nei riguardi di cittadini e imprese, per conto delle pubbliche amministrazioni. Il cittadino, una volta effettuata la procedura di autenticazione con uno solo dei soggetti coinvolti, potrà fruire di tutti i servizi online forniti dagli aderenti al network, in particolare pubbliche amministrazioni. Il 28 luglio 2015, con la Determinazione n. 44/2015, sono stati emanati i quattro regolamenti attuativi previsti dall'articolo 4, commi 2, 3 e 4, del DPCM 24 ottobre 2014. Il regolamento che norma le modalità di accreditamento entrerà in vigore il 15 settembre 2015, data a partire dalla quale i soggetti interessati potranno presentare domanda di accreditamento all'Agenzia. Con l'emanazione dei suddetti regolamenti il Sistema Pubblico di Identità Digitale diviene operativo.

[29] Reg. UE 910/2014 del 23 luglio 2014 del Parlamento europeo e del Consiglio, noto con l'acronimo di "*eIDAS*" (elettronic IDentification Authentication and Signature) che abroga la Direttiva UE del 1999 sulle firme elettroniche

"*insieme di dati che consente di stabilire l'identità di una persona fisica o giuridica, o di una persona fisica che rappresenta una persona giuridica*".

Il regolamento europeo quindi, come le altre fonti normative indicate, non fa menzione di un concetto di identità digitale, che in esso non può perciò trovare un riferimento esaustivo. Cionondimeno esso risulta utile per capire quali possono essere i dati che, all'interno di un sistema informatico o telematico, permettono di individuare univocamente un soggetto e che perciò concorrono a delineare un'identità nel mondo digitale: può trattarsi sia di dati forniti da un *service provider* per l'autenticazione in un network al fine di godere di beni e servizi sia di dati propriamente sensibili, utili per identificare una persona nel mondo reale. A ben vedere, per quanto possa destare perplessità il riferimento all'ipotesi di "utilizzare" un'identità altrui parallelamente alla possibilità di "rubarla", il legislatore ha voluto conferire un sostrato di materialità all'identità personale nel cyberspazio, al precipuo fine di tutelarla in una dimensione che ha una vita propria e regole proprie. I *social media* sono diventati sempre più mezzi privilegiati per intrecciare e mantenere relazioni, ma contemporaneamente costituiscono strumenti di sviluppo della personalità, poiché in essi l'individuo si esprime e contribuisce a "scrivere chi è", diffondendo così una proiezione digitale di sé, rafforzata da uno stile espressivo ed un determinato bagaglio lessicale e culturale: parallelamente alla smaterializzazione dell'individuo si assiste alla sua digitalizzazione attraverso la creazione di un'identità-maschera (persona deriva dal greco "*pròsopon*" che significa maschera) che nello spazio virtuale è assolutamente "viva e reale" e necessita di protezione rispetto a tutte le sue possibili estrinsecazioni: per questo alcuni autori hanno parlato di "giuridificazione dell'identità", sottolineando così che l'identità personale non è da intendersi come qualcosa di ontologicamente definito ma ha confini sempre nuovi e mobili, legati allo sviluppo degli strumenti di espressione ed interazione[30].

Non vi è il riferimento ad un entità definita come i dati d'accesso ad un sistema (*username* e *password* o PIN di solito), poiché la *ratio* dell'integrazione

[30] "*Il furto di identità digitale: una tutela patrimoniale della personalità*" di G. Malgieri, in "*La giustizia penale nella rete. Le nuove sfide della società dell'informazione nell'epoca di Internet*", a cura di R. Flor, D. Falcinelli, S. Marcolini, ed. DiPLaP, 2014.

normativa del 2013 è diversa da quella che ha ispirato le norme definitorie extrapenali; inoltre ciò limiterebbe troppo la portata applicativa dell'aggravante, rischiando di creare vuoti di tutela anche alla luce degli sviluppi tecnologici e risultare presto desueta.

Perciò l'opzione migliore è considerare la nozione come concetto atecnico, da interpretarsi in maniera ampia e teleologicamente orientata: in realtà ciò che rileva ai fini dell'applicazione della disposizione penale è la proiezione in ambito virtuale della persona, intesa come l'insieme di qualsiasi tipo di dati od elementi *latu sensu* sensibili in grado di creare nella Rete un univoca identità, quindi riconducendo direttamente ad una e una sola persona fisica quella maschera creata nel cyberspazio. La frode informatica così aggravata è posta a presidio, in particolare, dell'utente sprovveduto e inesperto, il quale non possiede gli strumenti conoscitivi e tecnologici per arginare gli attacchi fraudolenti di chi si spaccia per lui stesso nella rete. In tal modo si vuole costruire un sistema di tutela che, da un lato, aumenti la fiducia dei cittadini nell'utilizzazione dei servizi online e ponga un argine al fenomeno delle frodi realizzate – soprattutto nel settore del credito al consumo – mediante il furto di identità; dall'altro, agevoli altresì una regolazione del mercato, di modo tale da espellere chi lo droga con tecniche fraudolente.

I tentativi definitori di tale nozione in sede extrapenale sono sicuramente apprezzabili ma a ben vedere sono creati *ad hoc* rispetto ai provvedimenti nei quali sono inseriti e non sempre riescono a cogliere appieno la *ratio* sottesa all'introduzione dell'aggravante nel sistema penale: ciò avviene nel caso di identità digitale intesa come processo di identificazione informatica, limitandosi in tal caso la nozione al momento della validazione in un sistema di un insieme di dati al fine di individuare all'interno di esso un soggetto utente di determinati servizi.

La definizione che ad oggi può risultare più utile è quella introdotta con il DPCM del 2014, se svincolata da quegli elementi che la rendono settoriale e specifica, in primis il riferimento alla verificazione dei dati raccolti e registrati secondo le modalità del decreto stesso e dei regolamenti attuativi: in tal modo per identità digitale ai fini penali si intenderebbe la mera *rappresentazione informatica della*

corrispondenza biunivoca tra un utente e i suoi attributi identificativi, dando così spazio ai pratici del diritto di individuare questi ultimi in qualsiasi tipo di elemento, non solo quello che permette direttamente l'identificazione in un sistema (*id est*, i dati di autenticazione).

Rimane comunque da rilevare la mancanza e la acuta necessità di una disposizione definitoria ai fini penali, che possa creare una convergenza sul concetto di identità digitale alla luce della *ratio* dell'introduzione normativa del 2013, trovando un equilibrio fra le varie definizioni settoriali proposte e soprattutto individuando dei confini precisi per lo stesso.

Una possibile definizione di identità digitale potrebbe essere sviluppata nei seguenti termini: "*Per identità digitale s'intende qualsiasi insieme di informazioni personali, dati sensibili ovvero credenziali d'accesso di cui una persona abbia la piena ed esclusiva disponibilità in un sistema informatico o telematico e che permettono di individuare tale soggetto nel sistema stesso, creando una corrispondenza biunivoca con un'identità personale. Costituiscono identità digitale un profilo presente sui media sociali, un blog, un sito web, l'account di una e-mail o una p.e.c., una firma digitale o un sistema operativo online*".

Dal punto di vista delle condotte, l'aggravante introdotta nel 2013 ha subito una modifica non di poco conto durante i lavori di conversione del decreto legge: al posto del riferimento alla "*sostituzione di identità digitale*", la condotta è stata sdoppiata in due *species*, quella di furto e quella di indebito utilizzo. Il Parlamento ha voluto così tenere in debita considerazione i rilievi mossi soprattutto dai giudici di legittimità, i quali sottolineavano l'ambiguità della locuzione contenuta nell'art. 9 D.L. n. 93/2013, la quale "*formalmente evoca piuttosto che l'indebito utilizzo dell'identità, la sua surrogazione con altra al fine di accedere ai dati raggiungibili con quella sostituita e cioè fattispecie diversa e ben più specifica*" del caso di accesso abusivo ad un sistema attraverso l'utilizzo indebito di dati, "*ma di dubbia rilevanza*"[31].

Con la versione definitiva dell'aggravante in esame, il legislatore ha optato per una descrizione forse carente dal punto di vista della tecnica giuridica, data la materiale impossibilità di rubare o utilizzare un'identità quasi che fosse un'entità

[31] Rel. Cass. n. III/01/2013, Roma, 22/08/2013.

tangibile, ma molto attenta nel togliere ogni dubbio rispetto alla maggiore offensività di entrambe le modalità operative: la nozione di "sostituzione di identità digitale" contenuta nel decreto legge rischiava di creare disparità di trattamento o, peggio, vuoti di tutela in tutti quei casi limite in cui l'agente non impersonifica un altro soggetto bensì ha la legittima disponibilità di dati di terzi, i quali li hanno a lui affidati a determinati fini, e li sfrutta abusando di tale posizione per un tornaconto personale e recando loro danno.

Il legislatore quindi ha scelto – come nella descrizione della condotta fraudolenta al comma 1 – una definizione che può risultare sovrabbondante, mosso dall'intento di non escludere condotte magari diverse dal punto di vista delle concrete modalità operative ma simili dal punto di vista della gravità dell'offesa, e le ha accomunate in un'unica circostanza aggravante proprio in ragione del *vulnus* dalle stesse causato al diritto di ciascun soggetto alla riservatezza e all'affidabilità delle relazioni nel *cyberspace*: il focus dell'attenzione è sul modo di apprensione dell'insieme dei dati che costituiscono l'identità digitale, *ex se* illecito nel caso di "furto", *contra iure* solamente nell'uso e a prescindere dalla modalità di apprensione relativamente alla seconda condotta. L'uso della congiunzione disgiuntiva "o" conferma l'autonomia applicativa di ciascuna condotta, essendo indifferente, ai fini della configurazione dell'aggravante in esame, se sia compiuta una o l'altra, o se vengano poste in essere contestualmente: il risultato è sempre e comunque la contestazione della stessa circostanza aggravante speciale.

La vaghezza del dato linguistico consente di includere nell'ambito operativo della nuova norma non solo quelle condotte a pieno titolo considerabili strumentali alla realizzazione del fatto tipico, ma anche le azioni di furto o utilizzo indebito di dati carpiti tramite *hackeraggio* – in tal caso risolvendosi in un "*alterazione del funzionamento del sistema*" – o attraverso un altro tipo di "*intervento senza diritto sui dati*", sempre purché a ciò segua causalmente un profitto con correlativo danno: in questi casi è possibile configurare autonomamente il delitto di frode informatica, essendo integrata la condotta tipica già nel momento di captazione indebita dei dati e perciò non è necessario richiedere un trasferimento illecito di denaro da un patrimonio ad un altro, come

intervento modificativo sulla struttura dei dati[32].

Per definire l'indebito utilizzo e il rapporto con la modalità operativa del furto, risulta necessario cercare riferimenti in sede extra-penale, data la mancanza di definizioni *ad hoc*: il primo di essi può essere trovato nell'art. 55 c. IX del D.lgs. n. 231 del 2007, nel quale si rinviene testualmente una fattispecie di indebito utilizzo, ma riferita a carte di credito o pagamento[33]. Si tratta di una condotta similare che la giurisprudenza di legittimità ritiene inglobare parzialmente anche la condotta di sostituzione di persona[34]: tuttavia non si può tacere il fatto che in questo caso l'oggetto materiale dell'indebito utilizzo è un'entità tangibile e materiale, perciò mal si presta a definire la locuzione così come prevista dalla circostanza aggravante in commento.

Ciò di cui senza dubbio è possibile avvalersi sono i criteri ermeneutici elaborati per l'applicazione della norma del 2007: quindi si ritiene necessario avere la prova della consapevolezza dell'assenza del consenso del legittimo titolare dei dati; l'indebito utilizzo può ricorrere anche nel caso di mero uso difforme dalle condizioni stipulate in accordo con il titolare stesso[35]; infine vi è la possibilità di

---

[32] "*Il furto di identità digitale: una tutela patrimoniale della personalità*" di G. Malgieri, in "*La giustizia penale nella rete. Le nuove sfide della società dell'informazione nell'epoca di Internet*", a cura di R. Flor, D. Falcinelli, S. Marcolini, ed. DiPLaP, 2014.

[33] L'articolo dispone quanto segue: "*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, è punito con la reclusione da uno a cinque anni e con la multa da 310 a 1.550 euro. Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per altri, falsifica o altera carte di credito o di pagamento o qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, ovvero possiede, cede o acquisisce tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi*".

[34] Cass. Pen., sez. V, sent. n. 24816 del 6/06/2003, *Ferruti*, secondo cui "*il reato di indebita utilizzazione di carta di credito e di pagamento assorbe il reato di sostituzione di persona, di cui all'art. 494 c.p., ogni qual volta la sostituzione contestata sia posta in essere con la stessa condotta materiale integrante il primo reato. Ed infatti, l'ipotesi delittuosa dell'indebito utilizzo del mezzo di pagamento lede, oltre il patrimonio, anche la pubblica fede, mentre l'art. 494 c.p. contiene una clausola di riserva destinata ad operare anche al di là del principio di specialità ("se il fatto non costituisce un altro delitto contro la fede pubblica"). Sussiste, invece, concorso materiale fra gli stessi reati nel caso in cui la sostituzione sia stata realizzata con un'ulteriore e diversa condotta rispetto a quella che ha integrato l'altra fattispecie delittuosa*."(nel caso di specie, la S.C. ha annullato senza rinvio la sentenza in quanto non risultava la sostituzione di persona fosse stata realizzata con ulteriore comportamento rispetto a quello consistente nella mera utilizzazione indebita della carta)

[35] Trib. Milano, 8 novembre 2006, in *Giur. Merito*, 2012, 9, 1936, in cui si specifica come l'"*indebito utilizzo ricorre anche quando il consenso è prestato da parte del titolare dell'identità digitale violata, sempre che l'uso avvenga in modo difforme all'accordo convenuto col titolare stesso*".

esprimere il consenso all'uso dei dati altresì attraverso comportamenti concludenti.

Altro riferimento extrapenale che ci si è domandati se possa costituire un solido riferimento per la definizione di "indebito utilizzo" è l'art. 167 del codice della privacy, che rinvia a vari altri articoli *intra codicem*, la violazione dei quali costituisce reato[36]: si tratta in generale di sanzionare i casi nei quali operatori privati o enti pubblici economici procedano al trattamento di dati personali altrui senza un consenso pieno, circostanziato e documentato per iscritto da parte dell'interessato, se tali attività sono poste in essere con il precipuo fine di trarne profitto o di arrecare ad altri danno e "*se dal fatto deriva nocumento*". A ben vedere, il concetto di trattamento illecito di dati sembra più ristretto rispetto a quello di "indebito utilizzo", poiché delimitato nel campo applicativo da concetti definiti dallo stesso codice privacy. L'art. 23 del D.lgs. n. 196/2003 in esame, infatti, che rinvia alle informazioni di cui all'art. 13 da rendere obbligatoriamente all'interessato ai fini della liceità del trattamento, prevede tutta una serie di condizioni in base alle quali deve avvenire il trattamento stesso: fra le stesse informazioni, è fatto riferimento anche alle "*finalità specifiche e alle modalità del trattamento*", le quali perciò fungono da canone di giudizio della liceità dello stesso. L'abuso delle finalità concordate determina quindi un utilizzo indebito dei dati ai sensi della disciplina in materia di privacy, come tale sanzionabile ai sensi dell'art. 167 cod. privacy. Le operazioni di trattamento dati devono inoltre svolgersi nell'ambito di una attività commerciale o professionale: esiste infatti

[36] Art. 167 codice privacy: "*1. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 18, 19, 23, 123, 126 e 130, ovvero in applicazione dell'articolo 129, è punito, se dal fatto deriva nocumento, con la reclusione da sei a diciotto mesi o, se il fatto consiste nella comunicazione o diffusione, con la reclusione da sei a ventiquattro mesi*". *2. Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare ad altri un danno, procede al trattamento di dati personali in violazione di quanto disposto dagli articoli 17, 20, 21, 22, commi 8 e 11, 25, 26, 27 e 45, è punito, se dal fatto deriva nocumento, con la reclusione da uno a tre anni*.
Fra gli articoli cui la disposizione penale rinvia, particolare importanza riveste l'art. 23 che disciplina il Consenso al trattamento, a tenore del quale "*1. Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato. 2. Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso. 3. Il consenso è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 13* [quali in primis le modalità e finalità del trattamento stesso]*. 4. Il consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili.*"

all'art. 5 c. 3 la c.d. "eccezione domestica", la quale esonera dalla necessità del consenso tutti quelle ipotesi in cui il trattamento dei dati è effettuato da persone fisiche a fini esclusivamente personali. Il consenso non è altresì necessario (art. 24 lett. c) quando il trattamento riguardi dati "noti", provenienti da registri pubblici, elenchi, atti o documenti conoscibili da chiunque (per es. nome e cognome, che cionondimeno possono essere utilizzati per creare un falso profilo su un social network)[37]. Perciò la disposizione in commento non risulta applicabile nei casi di creazione di un profilo a nome altrui, utilizzando esclusivamente dati presenti in pubblici registri[38] ovvero dati pubblici mescolati con informazioni di fantasia.

Alla luce di queste considerazioni, appare evidente come il concetto di trattamento dati sia normativamente definito nei presupposti oggettivi e soggettivi nonché relativamente alle condizioni operative; l'espressione "indebito utilizzo" invece è volutamente più generale, in grado perciò di includere anche i casi suindicati che non troverebbero presidio nella normativa contenuta nel D.lgs. n. 196/2003, ovvero il trattamento dati in ambito esclusivamente privato e l'utilizzo di dati "pubblici". Se è vero che la condotta di trattamento illecito di dati è completamente inclusa nell'ipotesi di "utilizzo indebito di identità digitale", è anche vero però che il rapporto intercorrente fra la frode informatica complessivamente intesa e la fattispecie di cui all'art. 167 cod. privacy è alquanto complesso; vi sono infatti elementi come la diversità di bene giuridico[39] e requisiti specifici dell'una e dell'altra fattispecie[40] che depongono per un rapporto di specialità bilaterale per aggiunta.

In base a questa ricostruzione, le due fattispecie potrebbero concorrere se il

[37] La Corte di Cassazione ha ritenuto applicabile tale eccezione, ritenendo che non sussistesse il trattamento illecito di dati ai sensi dell'art. 167 cod. privacy in un caso di sostituzione di persona posto in essere utilizzando dati reperibili in "pubblici registri". Cass. Pen., sez. III, sent. n. 5728 del 15/02/2005.

[38] Cass. Pen., sez. III, sent. n. 5728 del 15/02/2005.

[39] L'opinione maggioritaria considera la fattispecie di frode informatica posta a tutela del patrimonio, mentre l'illecito trattamento di dati personali è norma posta a presidio del diritto alla riservatezza.

[40] La frode informatica è reato d'evento, perciò elemento costitutivo di cui è necessaria la verificazione sono l'ingiusto profitto e il correlativo danno altrui; nel trattamento illecito invece la tutela si aziona in via anticipata, dato che non è richiesto l'evento di danno bensì il dolo specifico di vantaggio o di danno. Il "nocumento" richiesto viene comunemente interpretato come condizione di punibilità intrinseca, non come elemento costitutivo del fatto tipico.

trattamento illecito fosse solo prodromico ad una frode informatica e distinto dalla stessa, magari all'interno della cornice del "*medesimo disegno criminoso*" ex art. 81 c.p., applicandosi in tal caso il cumulo giuridico. Il concorso non potrebbe configurarsi se il trattamento fosse pura modalità operativa attraverso cui l'agente realizza direttamente la frode informatica: si tratta di quei casi in cui esso non potrebbe essere scisso dalla condotta fraudolenta principale e verrebbe quindi sanzionato solo in quanto integrata la circostanza aggravante.
Tuttavia si tratta di una distinzione complessa da rinvenire sul piano operativo poiché non è sempre facile dal punto di vista delle azioni umani capire se si tratta di condotte autonome, solo connesse oppure se la condotta fraudolenta è una inscindibile.
Vi è poi un elemento nell'art. 167 che potrebbe far propendere per l'applicazione solamente della fattispecie di frode informatica perché più grave, vale a dire la clausola di riserva "*quando il fatto non costituisce più grave reato*": tuttavia anche su come sia necessario intendere quest'ultima si registrano opinioni divergenti, giacché la dottrina maggioritaria sostiene l'assenza di concorso – e la prevalenza della fattispecie più grave assorbente – ogniqualvolta la violazione della norma poi assorbita costituisce esclusivamente una modalità di commissione di altro e più grave reato, mentre la giurisprudenza ha richiesto che le due norme siano poste a presidio del medesimo bene giuridico. Nel caso in esame quindi non potrebbe rinvenirsi la prevalenza della fattispecie di cui all'art. 640-ter c.p., data la diversità di bene giuridico tutelato.
Per quanto riguarda più propriamente il furto di identità digitale, in sede di lavori parlamentari è stato asserito come sia necessario fare riferimento all'art. 30-bis del D.lgs. n. 141/2010[41], il quale definisce il furto d'identità come:

a) L'*impersonificazione totale*, ossia l'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

[41] Relazione della deputata A. D. Ferranti relatore per la II Commissione, anche a nome del deputato F. P. Sisto, relatore per la I Commissione, in sede di discussione sulle linee generali del disegno di conversione n. 1540-A, in www.camera.it.

l'utilizzo indebito di dati riferibili sia ad un soggetto in vita sia ad un soggetto deceduto;

b) L'*impersonificazione parziale*, ovvero l'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 lett. a)

Alla luce di tale rifermento però, si rischia di considerare l'indebito utilizzo di dati come condotta strumentale al furto d'identità e risulterebbe perciò difficile, da un lato, comprendere la formulazione dell'art. 9 della legge di conversione del 2013 che configura le due modalità d'azione in via alternativa, dall'altro la scelta di punire con la stessa severità una condotta complessa (il furto) e una condotta semplice (l'indebito utilizzo)[42].

Anche l'OCSE ha fornito una definizione di furto d'identità che corrobora questo orientamento: esso consisterebbe, tra l'altro, in un "*uso di informazioni personali in modo non autorizzato*", perciò anche per l'organizzazione internazionale l'indebito utilizzo costituirebbe una sottocategoria del furto d'identità[43].

Tuttavia, per riuscire a conservare un ambito applicativo autonomo a ciascuna modalità d'azione e dare quindi rilevanza pienamente disgiuntiva alla congiunzione "o" utilizzata dal legislatore, spunti interessanti sono forniti dalla dottrina di *common law* e dal centro studi delle Nazioni Unite[44]: entrambi gli orientamenti distinguono nettamente le due condotte, individuando il furto d'identità digitale nella mera apprensione di dati e l'utilizzo illecito come elemento costitutivo della frode d'identità. Vengono così poste le premesse per considerare l'indebito utilizzo di identità digitale come condotta alternativa al

[42] In questo caso sarebbe necessario considerare la congiunzione "o" come mezzo per meglio definire (come "ossia", "ovvero") il furto d'identità, al fine di introdurre una diversa denominazione per una condotta similare che deve essere senza dubbio alcuno inclusa nel raggio d'azione della norma.

[43] OCSE, "*Scoping Paper on Online Identity Theft*", 18 giugno 2008, Section I: "ID *theft occurs when a party acquires, transfers, possesses, or uses personal information of a natural or legal person in an unauthorised manner, with the intent to commit, or in connection with, fraud or other crimes*".

[44] UN IEG, "Results of the second meeting of the Intergovernmental Expert Group to prepare a study on Fraud and the criminal misuse and Falsification of identity": "[…] *scenarios in which genuine identity information or documents are actually taken or misappropriated are described as «identity theft», while scenarios in which identities were used to deceive others are referred to as «identity fraud»*".

furto, in quanto “frode” all’identità, nella quale i dati vengono sfruttati all’insaputa o contro la volontà del titolare, pur avendone questi magari la legittima disponibilità.

Le condotte risultano pienamente alternative, ricalcando la distinzione tecnica 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).

Non potendo consistere comunque il furto d’identità in un mero possesso di dati altrui bensì in una vera e propria azione di sostituzione di persona – come testimonia anche il rinvio operato in sede parlamentare al D.lgs. n. 141/2010 e al concetto di “impersonificazione”– l’interpretazione maggiormente convincente della nuova aggravante è quella secondo la quale l’effetto finale derivante da entrambe le modalità operative è sostanzialmente una sostituzione di persona, possibile nel primo caso attraverso un’apprensione illecita di dati personali; nel caso della seconda modalità invece compiuta con un uso “deviato” o “non autorizzato” di dati raccolti in maniera lecita (dati posseduti lecitamente per altri scopi, dati noti o presenti in pubblici registri).

Recentemente, autorevole dottrina ha ravvisato nell’introduzione del comma 3 art. 640-ter c.p. un interessante spiraglio per slegare la frode informatica aggravata da sostituzione di identità digitale dalla stretta concezione patrimonialistica che da sempre ha ispirato l’esegesi dell’ipotesi base.

L’identità personale si sta sempre più frazionando in molteplici proiezioni digitali che, andando ben oltre i semplici dati d’accesso ad un sistema, richiedono all’ordinamento un intervento di presidio mirato: nasce così un complesso “patrimonio umano digitale”, formato da chiavi d’accesso ad un patrimonio materiale o a determinati servizi, strumenti per un guadagno commerciale (i dati in sé considerati), domicilio virtuale, estrinsecazione della proprietà intellettuale e strumento per i rapporti sociali (online), il quale necessita di una forma di tutela combinata, che guardi sia al patrimonio sia alla persona.

Il primo vero esempio di questo tipo di tutela è l’innovazione legislativa del 2013: il furto o indebito utilizzo di identità digitale può costituire non soltanto condotta strumentale alla realizzazione del fatto tipico, ma anche modalità

stessa del fatto tipico, purché vi sia un profitto associato ad un depauperamento del patrimonio della vittima. In altri termini, viene utilizzata l'identità di un soggetto come grimaldello per un tornaconto personale, che può non avere consistenza direttamente patrimoniale.

Valorizzando a pieno il riferimento all'identità digitale, è possibile estendere l'applicazione del reato di frode informatica attraverso un ripensamento del concetto stesso di "patrimonio": tale nozione non dovrebbe più essere equiparata concettualmente ad un'entità materiale, ma dovrebbe essere intesa come "patrimonio personalissimo", "*contrappeso in termini di riservatezza e libertà negoziale del guadagno concreto che gli operatori del web ricevono a fronte di un "bene" immateriale ma economicamente rilevante: i dati personali*".

Il consumatore diventa così titolare di un monopolio passivo (in quanto unico soggetto che possiede e legittimamente può far uso dei dati) e attivo (in quanto unico soggetto che può modificare, eliminare o creare nuovi dati nel tempo), la lesione del quale senza dubbio costituisce un danno economico: sulla base di queste premesse però si tratterebbe di un danno solo eventuale, dipendente dal potenziale uso a fini di lucro dei dati personali (per es. vendita a operatori del web), come tale difficilmente provabile.

Vi è un'altra strada percorribile, più agevole, che è poi quella prescelta dal legislatore francese: in una visione più armonica e univoca delle molteplici istanze di tutela, l'ordinamento francese sanziona la frode informatica collocandola sì tra i delitti contro il patrimonio (*Livre III, Des crimes e delictes contre les biens*), ma considerando come bene leso l'integrità dei dati informatici e della struttura informatica di un programma o sistema operativo *(Titre II, Chapitre III, des atteintes aux systèmes de traitement automatisé de données)*[45]. Perciò anche la lesione di un *account* potrebbe integrare la fattispecie, in quanto "bene" nella titolarità della vittima: i "dati informatici" verrebbero considerati a pieno titolo parte del patrimonio economico della persona e potrebbero così godere della severa protezione per questo predisposta dal nostro ordinamento.

[45] L'alterazione di dati è vista come aggravante speciale della norma di frode informatica, che così come è strutturata coincide sostanzialmente con la nostra fattispecie di accesso abusivo ad un sistema informatico ex art. 615-ter c.p.

Un'impostazione di questo genere avrebbe il merito di rendere la tutela più aderente alla fenomenologia degli illeciti informatici e più facilmente attivabile. Nel nostro ordinamento, tuttavia, si scontra con il principio di legalità in materia penale e con la molteplicità di fattispecie introdotte senza una visione organica a protezione di vari beni giuridici singolarmente ritenuti meritevoli di protezione. Questa varietà, cui consegue un'ampia discrezionalità nella scelta della norma da parte degli apparati giudiziari, causa una profonda frammentazione ed inefficacia della tutela: la frode informatica è stata introdotta a tutela del patrimonio nel senso più squisitamente economico del termine, essendo affiancata da altre fattispecie come l'accesso abusivo ad un sistema informatico (art. 615-ter c.p.) o il trattamento illecito di dati personali (art. 167 cod. privacy) che intervengono a tutela di altri interessi. Sul piano pratico però tale frammentazione conduce a situazioni molto pericolose, essendo da un lato frequentissime le ipotesi di concorso con conseguente raggiungimento di eccessi sanzionatori[46], dall'altro non conferendo una tutela effettiva ed efficace all'unico bene che realmente necessita di tutela, l'identità dell'individuo e il suo patrimonio di dati identitari.

Nel complesso, l'aggravante introdotta nel 2013 ha molti pregi, fra cui quello di creare l'occasione per una riflessione innovativa sul *modus operandi* della tutela penale in ambito informatico; si tratta del primo reale tentativo di implementare in un'unica norma la tutela della proiezione della identità personale in ambito virtuale combinata alla tradizionale tutela del patrimonio, creando un presidio composito più rispondente alle peculiarità del fenomeno in esame.

Tuttavia permane qualche criticità: in primis la sottrazione di dati deve necessariamente riguardare una identità reale, di una persona fisica o di una persona giuridica, quale presupposto del reato stesso. Non è possibile contestare l'aggravante in commento nel caso di utilizzo di dati di più soggetti reali per creare un profilo fittizio nella rete ovvero nel caso di profili realizzati con un misto di dati di persone reali e dati di fantasia. Proprio l'utilizzo sempre

[46] Anche applicando la disciplina del cumulo giuridico ex art. 81 c.p. la pena risultante andrebbe dai 2 anni (minimo edittale dell'art. 640-ter c. 3 c.p.) ai 18 anni (i 6 anni previsti come massimo edittale ex art. 640-ter c. 3 c.p. aumentati del triplo), sanzione forse troppo alta per un reato non così offensivo.

più diffuso, specie sui social network, di nickname di fantasia ovvero di profili riferiti a persone inesistenti, che rendono particolarmente difficoltoso ricondurre il reato a una persona fisica certa. Altro elemento critico è costituito dalla pluralità dei modi con i quali è possibile acquisire i dati personali. È da sfatare la percezione che solo chi "frequenta" i media sociali o naviga in rete può incappare in questi problemi. Basti pensare alla diffusa abitudine di alcuni negozi che, a fronte del pagamento di prodotti con assegno bancario, richiedono un documento di identità di cui spesso viene fatta la fotocopia.
Infine altra complessa questione deriva dalla difficoltà di coordinamento del *novum* legislativo con le altre disposizioni poste a tutela delle varie proiezioni dell'identità personale in ambito informatico: l'intervento poco organico del legislatore, motivato dalle necessità contingenti di protezione, ha comportato una frammentazione della tutela dell'unico reale bene giuridico, l'identità personale digitale. L'operatore del diritto ha a disposizione una pluralità di fattispecie associate ad una – forse eccessiva – discrezionalità, con margini edittali piuttosto ampi (dai 2 ai 18 anni di reclusione) e la possibilità di configurare od escludere svariate ipotesi di concorso, stante la specialità reciproca che le caratterizza.

3.3 La frode del certificatore di firma elettronica: art. 640-quinquies c.p.

Già si è avuto modo di descrivere il contesto nel quale il legislatore ha deciso di introdurre nel nostro ordinamento un'ipotesi speciale dal punto di vista soggettivo rispetto alla tradizionale truffa: il Parlamento si stava occupando – forse un po' frettolosamente- sul finire della XV Legislatura della legge di ratifica della "Convenzione di Budapest sulla criminalità informatica" del 2001 e, nell'ambito di tale lavoro di recepimento e adattamento, optò per l'introduzione di due fattispecie completamente nuove, non affatto esecutive di obblighi pattizi, le quali puniscono violazioni della disciplina italiana concernente le firme elettroniche. Una di queste fu l'art. 640-quinquies c.p.[47], delitto proprio che ha

[47] L'altro fu l'art. 495-bis c.p. "*False dichiarazioni al certificatore*"

come soggetto attivo il certificatore di firma elettronica qualificata.

L'articolo in commento dispone quanto segue: "*Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro*."

Come già accennato, si tratta di una norma penale in bianco: il legislatore si è limitato a sanzionare penalmente violazioni *aliunde* previste[48]. In questo caso, il

[48] L'Art. 32 definisce gli "*Obblighi del titolare e del certificatore*":
"*1. Il titolare del certificato di firma è tenuto ad assicurare la custodia del dispositivo di firma e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri; è altresì tenuto ad utilizzare personalmente il dispositivo di firma.*
2. Il certificatore è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno a terzi.
3. Il certificatore che rilascia, ai sensi dell'articolo 19, certificati qualificati deve inoltre:
a) provvedere con certezza alla identificazione della persona che fa richiesta della certificazione;
b) rilasciare e rendere pubblico il certificato elettronico nei modi o nei casi stabiliti dalle regole tecniche di cui all'articolo 71, nel rispetto del decreto legislativo 30 giugno 2003, n. 196.
c) specificare, nel certificato qualificato su richiesta dell'istante, e con il consenso del terzo interessato, i poteri di rappresentanza o altri titoli relativi all'attività professionale o a cariche rivestite, previa verifica della documentazione presentata dal richiedente che attesta la sussistenza degli stessi;
d) attenersi alle regole tecniche di cui all'articolo 71;
e) informare i richiedenti in modo compiuto e chiaro, sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi e sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;
f) lettera soppressa dall'art. 22, D.lgs. n. 235 del 30 dicembre 2010.
g) procedere alla tempestiva pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri del titolare medesimo, di perdita del possesso o della compromissione del dispositivo di firma, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti abusi o falsificazioni, secondo quanto previsto dalle regole tecniche di cui all'articolo 71;
h) garantire un servizio di revoca e sospensione dei certificati elettronici sicuro e tempestivo, nonché garantire il funzionamento efficiente, puntuale e sicuro degli elenchi dei certificati di firma emessi, sospesi e revocati;
i) assicurare la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;
j) tenere registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato dal momento della sua emissione almeno per dieci anni anche al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;
k) non copiare, né conservare, le chiavi private di firma del soggetto cui il certificatore ha fornito il servizio di certificazione;
l) predisporre su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione, tra cui in particolare gli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie; dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in

riferimento principale corre al Codice dell'Amministrazione Digitale (D.lgs. n. 82 del 7 marzo 2005), nel quale sono previsti dettagliatamente vari obblighi cui è soggetto il certificatore di firma elettronica; il medesimo codice inoltre fornisce una definizione normativa del concetto di "firma elettronica", utile per delimitare la nozione di certificatore in ambito penale e conferire determinatezza alla fattispecie[49]. Si è osservato in dottrina che il rinvio al codice Amm. Digit. suscita perplessità in ordine alla collocazione sistematica dell'art. 640-quinquies c.p. e alla rubrica che si esprime in termini di "frode", poiché la maggior parte delle condotte previste dall'art. 32 non sono connotate da un intento fraudolento di induzione in errore (art. 640 c.p.) o dalla manomissione di sistema o contenuto informatico (art. 640-ter c.p.)[50].

Dal punto di vista della condotta, quindi, si tratta di una disposizione assolutamente aperta, che può astrattamente essere chiamata in causa ogniqualvolta il certificatore commetta una violazione di un obbligo previsto

---

linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio e il certificatore;

m) utilizzare sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza. Su richiesta, elementi pertinenti delle informazioni possono essere resi accessibili a terzi che facciano affidamento sul certificato;

m-bis) garantire il corretto funzionamento e la continuità del sistema e comunicare immediatamente a DigitPA e agli utenti eventuali malfunzionamenti che determinano disservizio, sospensione o interruzione del servizio stesso;

4. Il certificatore e' responsabile dell'identificazione del soggetto che richiede il certificato qualificato di firma anche se tale attività e' delegata a terzi.

5. Il certificatore raccoglie i dati personali solo direttamente dalla persona cui si riferiscono o previo suo esplicito consenso, e soltanto nella misura necessaria al rilascio e al mantenimento del certificato, fornendo l'informativa prevista dall'articolo 13 del decreto legislativo 30 giugno 2003, n. 196. I dati non possono essere raccolti o elaborati per fini diversi senza l'espresso consenso della persona cui si riferiscono."

[49] Il codice dell'Amministrazione Digitale offre, all'art. 1 e segg., alcune definizioni: alla lett. q) quella di *firma elettronica*: "l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica"; alla lett. r) quella di *firma elettronica qualificata*: "firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario e la sua univoca autenticazione informatica, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare si i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma, quale l'apparato strumentale usato per la creazione della firma elettronica".

[50] G. Amato, "*Danneggiamento*" in Codice penale – Rassegna di dottrina e giurisprudenza, di G. Lattanzi, Giuffré, 2010; in senso critico anche L. Picotti, "*La ratifica delle Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*", 2008

dalla legge[51]: questo è il rischio di ogni norma penale "in bianco" ed è proprio per questo che sono così osteggiate in dottrina. La disposizione non ha una carica offensiva propria, non prevede in termini tassativi una condotta contraria all'ordinamento alla quale segue, se realizzata, la comminatoria di una sanzione, quindi il cittadino non può sapere *ex ante* con chiarezza quale sarebbe la regola di comportamento da osservare in concreto: viene semplicemente prevista una sanzione che può essere applicata senza dei limiti ben determinati a tutte le condotte che integrano gli elementi previsti dalle disposizioni di rinvio (spesso generico, come nel caso in esame), creandosi quindi una forte tensione con il principio di tassatività-determinatezza cui sempre deve essere orientato il diritto penale[52]. Non è richiesto alcun evento consumativo di *lesione* patrimoniale, come è invece quello duplice di "ingiusto profitto con altrui danno" previsto dall'art. 640 c.p. e riprodotto negli artt. 640-bis e 640-ter c.p.

L'unico vero requisito ulteriore previsto dalla fattispecie penale, rispetto alle corrispondenti disposizioni sanzionatorie previste in sede extrapenale, è il dolo specifico: la sanzione penale si cumulerà con la sanzione civile solamente nel caso in cui l'agente abbia commesso il fatto con il preciso fine di "*procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno*". Tale requisito soggettivo è previsto in via alternativa ed è fondamentale e dirimente, perché permette di apprestare un presidio penale anticipato nel caso in cui si verifichi la violazione ivi prevista: il legislatore, consapevole della maggiore offensività della condotta posta in essere dal certificatore ed il ruolo svolto dallo stesso, introduce una sanzione penale in via anticipata rispetto alla effettiva causazione di un danno con profitto altrui, che è elemento tipico della truffa tradizionale[53].

---

[51] Il riferimento alla legge è altresì da intendersi in senso ampio come legge ed atti aventi forza di legge, incluse le leggi regionali nel territorio in cui si applicano

[52] Vari autori denunciano l'incostituzionalità delle norme penali "in bianco": F. Bricola, "*Legalità e crisi, l'articolo 25 c. 2 e c. 3 Cost., rivisitato alla fine degli anni '70*", in Quest. Crim. 1980, p. 193; G. Carboni, "*L'inosservanza dei provvedimenti dell'Autorità*", Milano, 1970; in senso critico, G. Fiandaca - E. Musco, "*Diritto penale, Parte generale*", Zanichelli, VI ed.; M. Grotto, "*Reati informatici e convenzione cyber crime. Oltre la truffa e la frode informatica: la frode del certificatore*", in Dir. inform., 2009, pag. 145

[53] Recentemente, parte della dottrina si è espressa in maniera piuttosto critica riguardo alla figura del dolo specifico, con particolare riguardo a quelle fattispecie nelle quali esso contribuisce in maniera decisiva a rendere illecito penalmente un fatto di per sé lecito o già sanzionato in via extrapenale: il rischio è di connotare l'incriminazione in senso marcatamente

Condivisibilmente, recente dottrina ha sottolineato che la disposizione vada integrata in via interpretativa con un evento non scritto, consistente nel rilascio di un certificato qualificato che non contenga i requisiti richiesti dalla legge: solo così è possibile porre un argine alla portata applicativa della norma, riferendola esclusivamente ai casi di concreto pericolo per l'interesse tutelato[54].

L'art. 640-quinquies c.p. si pone quindi in rapporto di specialità con la fattispecie di cui all'art. 640 c.p., stante la condivisione della maggior parte degli elementi costitutivi e la specificazione operata attraverso l'anticipazione della tutela, determinata dalla trasformazione dell'evento di danno in elemento soggettivo che l'agente deve raffigurarsi nel momento in cui pone in essere la violazione, ma di cui non è necessaria l'obiettiva realizzazione.

Nel disegno di legge originario, la sanzione era incomprensibilmente prevista in via alternativa (reclusione o multa), diversamente dalla truffa tradizionale: tale illogica situazione è stata corretta in sede di approvazione con la previsione cumulativa delle pene. Desta però qualche perplessità la mancata previsione del minimo edittale rispetto a quanto previsto nell'art. 640 c.p.[55]: la *ratio* giustificatrice della fattispecie, inserita allo specifico fine di sanzionare anche penalmente il certificatore di firma elettronica che profitta illegittimamente del suo ruolo, indica che la carica offensiva viene percepita come più alta rispetto all'ipotesi base, stante la responsabilità e il ruolo di "garante" in senso lato ricoperti dal soggetto attivo.

Perciò risulta difficile comprendere poi un trattamento sanzionatorio seppur lievemente *in melius* rispetto alla truffa, tipico reato del *quisque de populo*.

Forse sarebbe stata più opportuna una maggiore personalizzazione della sanzione rispetto agli obblighi incombenti sul certificatore, con la previsione di sanzioni accessorie applicate *ex lege* come la sospensione dell'attività di

---

soggettivo, in contrasto con la concezione di diritto penale come *extrema ratio* e con la concezione di reato come fatto effettivamente offensivo di un bene protetto e non come un atteggiamento psicologico. L. Picotti, "*Il dolo specifico*", Milano 1993, M. Gelardi, "*Il dolo specifico*", Cedam, Padova.

[54] M. Grotto, *op.cit.*, in Dir. inform., 2009, pag. 149

[55] Nell'ipotesi tradizionale di truffa è previsto un minimo edittale di 6 mesi; nella fattispecie in esame, non essendo previsto un minimo edittale, si applica il limite minimo di 15 giorni previsto in via generale dall'art. 23 c.p.

certificazione ovvero la pubblicazione della sentenza di condanna[56], dotate di maggiore deterrenza ed effettività.

Si noti infine che la disposizione penale può essere applicata solo al certificatore "qualificato", cioè solo al certificatore che presta i propri servizi rispetto ad un documento contenente i requisiti previsti dall'art. 28 del D.lgs. n. 82/2005: la troppa aderenza alla fonte normativa extrapenale comporta il rischio di non vedere la sostanziale offensività di situazioni analoghe e conseguentemente di non poter apprestare una tutela penale solamente perché mancano dei requisiti previsti da una normativa di settore con propria *ratio* giustificatrice.

[56] In verità, la sanzione accessoria della pubblicazione della sentenza è stata introdotta nel 2010 ma in via solo facoltativa con l'art. 32-bis nel Codice dell'Amministrazione Digitale, nei casi di malfunzionamento non comunicato a DigitPA nel sistema che determinino un disservizio o un'interruzione di servizio.

Capitolo IV: Rapporto con altre fattispecie di "frode"

4.1: Frode informatica e art. 55 comma IX del D.lgs. n. 231/2007

"*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, e' punito con la reclusione da uno a cinque anni e con la multa da 310 a 1.550 euro. Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per altri, falsifica o altera carte di credito o di pagamento o qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, ovvero possiede, cede o acquisisce tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi".*

La fattispecie di indebito utilizzo delle carte di credito o di pagamento fu introdotta per la prima volta nel 1991 con la legge n. 197 recante "*provvedimenti urgenti per limitare l'uso del contante e dei titoli al portatore nelle transazioni e prevenire l'utilizzazione del sistema finanziario a scopo di riciclaggio*": si trattava di una disposizione in parte distonica rispetto al contenuto generale della legge e alla sua ispirazione a contrastare il riciclaggio di denaro di provenienza illecita, stante la sua vocazione privatistica alla tutela del patrimonio.

La medesima fattispecie è poi confluita nel d.lgs. n. 231 del 2007, con cui il Parlamento, dando attuazione alla Direttiva 2005/60/CE concernente la prevenzione dell'utilizzo dei proventi di attività criminose nel sistema finanziario a scopo di riciclaggio e di finanziamento del terrorismo nonché della Direttiva 2006/70/CE che ne reca misure di esecuzione, ha tentato di conferire alla materia una disciplina organica e completa.

Come spesso accade, la necessità dell'introduzione della normativa in esame è stata rinvenuta nell'inadeguatezza della disciplina vigente ante 1991: in particolare, se l'abuso delle carte di credito da parte di terzi tramite artifizi o raggiri poteva essere ricondotto alla fattispecie di truffa, nel caso di utilizzo di

carte magnetiche[1] era molto più difficile contestare il delitto di cui all'art. 640 c.p., dato che mancava il requisito fondamentale dell'induzione in errore di "taluno". Molta parte di giurisprudenza, al fine di dare una risposta effettiva alle pressanti esigenze di repressione penale, aveva scelto di applicare in questi casi la norma sul furto, eventualmente aggravato dall'utilizzo di mezzi fraudolenti[2]: tuttavia tale orientamento incontrava varie critiche, essendo volontaria la consegna sia del denaro allo sportello automatico sia dei beni acquistati attraverso l'uso del sistema POS. Dunque mancava in questi casi l'elemento dell'impossessamento della *res* contro la volontà del legittimo titolare. Alcune ricostruzioni giurisprudenziali, al fine di contestare il furto, ravvisavano nella carta di pagamento una chiave utile a procurarsi l'accesso al denaro altrui: tale assimilazione, se poteva risultare anche plausibile nel caso di prelievo allo sportello automatico, risultava del tutto inadeguata nelle ipotesi di utilizzo della carta per acquisti presso i c.d. POS, stante l'apparente legittimazione dell'utente[3].

Anche le condotte di contraffazione e alterazione delle carte magnetiche faticavano a trovare una risposta sanzionatoria, tanto che a volte il giudice era costretto a definire il fatto "penalmente irrilevante": ad esse non era possibile applicare le disposizioni in materia di falsità documentali, dato che non pareva potersi ricondurre alla nozione di "documento" accolta da dottrina e giurisprudenza maggioritarie la carta magnetica[4].

La fattispecie introdotta nel 1991 ha perciò colmato vuoti di tutela emersi con la

---

[1] Comunemente conosciute anche come carte di debito, per mezzo delle quali è possibile prelevare denaro in ogni sportello bancomat, conoscendo il codice di identificazione associato alla carta: ciò comporta l'addebito immediato sul conto corrente del titolare della carta del prelievo effettuato e degli eventuali costi annessi. Oggi esistono anche carte di credito a banda magnetica e carte "miste", le quali permettono all'utente di sfruttarle sia come strumento di pagamento sia come carta di credito.

[2] Cass. Pen., sez. II, sent. n. 1162 del 7/12/1989, "*Maiello*", nella quale la Cassazione ha rinvenuto la fattispecie di furto aggravato dall'impiego di mezzi fraudolenti nella sottrazione di banconote da uno sportello bancario di prelievo automatico realizzato con una falsa carta "Bancomat". La giurisprudenza non era in realtà unanime: si registrano infatti anche pronunce di irrilevanza penale del fatto, come Tribunale di Roma, 17 maggio 1991, "*Di Fiore*".

[3] C. Pecorella, *op.cit.*

[4] Documento è tradizionalmente "*qualcosa che fa conoscere qualcos'altro*", supporto avente quindi capacità rappresentativa di un fatto o di un atto. La carta magnetica non rappresenta visivamente un contenuto, dato il carattere "invisibile" ad occhio nudo delle informazioni registrate sulla banda magnetica. F. Carnelutti, "*Documento – teoria moderna*", in Nov. Dig. It., vol. VI, Torino, 1957, 85 ss..

diffusione sistematica dei metodi di pagamento alternativi al denaro contante: essa contempla diverse condotte illecite che vengono equiparate dal punto di vista dell'offensività e trattate congiuntamente rispetto al trattamento sanzionatorio. Il legislatore ha previsto una sanzione moderatamente più grave rispetto a quella prevista per la frode informatica e per la truffa per tutta una serie di condotte anche eterogenee fra loro ma considerate di pari gravità, il cui oggetto materiale sono *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.*

Con questa formula alquanto omnicomprensiva – data la clausola generale posta alla fine dell'elencazione – vengono indicati tutti quei metodi di pagamento alternativi al denaro contante, i documenti nominativi, che possono essere utilizzati all'interno degli esercizi convenzionati con il "Sistema nazionale di terminali nei punti di vendita" (POS), nonché quegli strumenti con cui si è reso possibile prelevare denaro contante ai distributori automatici di banconote, tramite l'identificazione attraverso un codice P.I.N. (personal identification number) associato alla carta stessa. La genericità della dizione "*documento analogo*" permette di includere nella fattispecie ogni nuova e più sicura tipologia di strumento inventata, che svolga la medesima funzione di quelli espressamente citati: il primo esempio sono certamente le carte a microprocessore (*microchip*), evoluzione delle carte magnetiche, che svolgono sempre la funzione di carta di credito o carta "bancomat". Nella definizione di carte di pagamento rientrano anche le carte di credito telefonico, le ricariche telefoniche e la tessera «Viacard», tutti documenti che autorizzano il titolare a ricevere beni e servizi con addebito virtuale della prestazione ricevuta[5]; si registra qualche divergenza d'opinione relativamente alle carte prepagate, documenti che non sono nominativi ma che possono essere utilizzate come metodo di pagamento negli esercizi convenzionati POS o come strumento di prelievo di denaro (fino alla disponibilità della carta stessa).

Per tracciare con successo i confini dell'oggetto materiale – che poi diventano i

[5] "*È configurabile il reato di cui all'art. 12, D.l. 3 maggio 1991, n. 143, nella condotta di chi si avvalga, per la ricarica del proprio telefono cellulare, di numeri di codice tratti da schede di illecita provenienza, all'uopo manomesse*", Cass. Pen., sez. II, sent. n. 41451 del 23/09/2003.

reali confini applicativi della norma, data l'ampiezza delle condotte – è opportuno seguire il canone interpretativo teleologico. Precedentemente si è cercato di analizzare l'oggettività giuridica della fattispecie in commento[6], soffermando l'attenzione sul processo di "privatizzazione" del bene giuridico che ha portato le Sezioni Unite a capovolgere l'orientamento prevalente anche fra le Sezioni Penali con la sentenza "*Tiezzi*" del 2001 confermandolo poi in pronunce successive: la situazione si è capovolta, da una prevalenza della concezione pubblicistica ancorata alla *ratio* della fattispecie, all'affermarsi dell'idea che la disposizione tuteli principalmente l'individuo e la sua sfera patrimoniale da possibili aggressioni di terzi[7]. Di conseguenza, le condotte possono avere come destinatario immediato tutti quegli strumenti che permettono al legittimo titolare di disporre del proprio patrimonio-denaro senza far circolare denaro contante, nonché gli strumenti che, per facilità d'uso e per capacità di trasferire elettronicamente fondi, possono incidere sulla stabilità e sulla trasparenza delle strutture deputate alle movimentazioni finanziarie

Si tratta di un reato comune, che può essere commesso da "*chiunque*", ma con una delimitazione offerta direttamente dalla disposizione: deve trattarsi di qualsiasi soggetto che non sia il titolare dello strumento di prelievo o pagamento.

Non si può parlare di reato proprio, pur essendo operata una limitazione dal punto di vista soggettivo, poiché l'ambito operativo della fattispecie non viene comunque circoscritto a soggetti titolari di una determinata qualifica o di un particolare *status* precisato dalla norma, o che possiedano un requisito necessario per la commissione dell'illecito: la disposizione esordisce enfaticamente con il pronome "*chiunque*", sottolineando la generalità dell'applicazione della stessa, e solo successivamente viene limitata nella portata ai soli *extranei* rispetto alla legittimazione all'uso della carta.

La disposizione perciò non trova applicazione per i casi di abuso di carta di pagamento o prelievo operati dal legittimo titolare della stessa, vale a dire colui che *ex contractu* può legittimamente disporne. La mancanza di una sanzione

[6] Vedi cap. II par. 1

[7] Note n. 30-31, fine cap. II par. 1; per un approfondimento anche *infra*.

penale prevista espressamente per tali ipotesi era già evidenziata con preoccupazione prima dell'introduzione normativa del 1991, essendo esclusa l'applicazione della fattispecie di truffa a causa dell'impossibilità di rinvenire l'induzione in errore di taluno: nemmeno con la ristrutturazione normativa del 2007 si è voluto positivizzare tale ipotesi, lasciando un pericoloso vuoto di tutela in tutti quei casi nei quali l'agente è identificabile proprio nella persona che ha ottenuto regolarmente il rilascio della carta di pagamento e approfitti della fiducia accordatagli dall'istituto di credito emittente[8]. Forzando un po' il dato normativo, una possibile risposta penale in tali ipotesi potrebbe essere oggi proprio l'art. 640-ter c.p., grazie alla diffusione sempre più crescente delle carte di pagamento e di prelievo a microprocessore, le quali potrebbero validamente essere assimilate ad un micro sistema informatico sul quale l'agente (titolare o meno della carta stessa) agisce; in tal caso sarebbe necessario riscontrare nel caso concreto la modificazione del funzionamento della carta, cui causalmente consegue il vantaggio patrimoniale con danno altrui. Potrebbe altresì astrattamente configurarsi la seconda condotta contemplata nella fattispecie di cui all'art. 640-ter c.p., ovvero l'intervento senza diritto sui dati contenuti in un sistema informatico o telematico, come può legittimamente essere considerato il circuito Bancomat o POS, se l'agente integra, modifica o elimina dati del sistema e ciò gli permetta di ottenere un illecito profitto.

Bisogna sottolineare comunque che si tratterebbe di un complesso iter argomentativo e di una tutela che interviene solamente *ex post factum*, data la struttura di reato d'evento della frode informatica, la quale richiede la disponibilità del profitto e la effettiva causazione del danno.

La struttura della fattispecie di cui all'art. 55 c. IX rispecchia la *volutas legislatoris* di creare un presidio atto a garantire una sanzione anticipata rispetto alla causazione di un possibile danno, sia esso considerato di tipo privatistico al patrimonio del legittimo titolare della carta ovvero di tipo pubblicistico all'affidabilità dell'attività finanziaria e dei trasferimenti di denaro: si tratta di un reato di mera condotta, che si perfeziona nel momento stesso nel quale

[8] Si pensi ad esempio ai casi di debito contratto per mezzo di carta di credito nella consapevolezza di non poterlo onorare successivamente o al quale non corrisponde una sufficiente disponibilità sul conto corrente nel caso di carta di debito.

l'agente pone in essere una delle varie attività previste, vale a dire fa uso in maniera indebita dello strumento di pagamento oppure lo falsifica o lo modifica rispetto al suo regolare funzionamento ovvero infine meramente si trova nella disponibilità di documenti, i quali sono stati precedentemente falsificati o alterati (situazione di possesso, cessione o acquisizione). Perciò le condotte che si è scelto di sanzionare penalmente sono quelle che si sostanziano in un abuso in senso lato di tali carte da parte di terzi, sia esso configurabile come utilizzo al di fuori di qualsiasi legittima facoltà della carta al fine di prelevare denaro contante o procurarsi beni e servizi ovvero come condotta volta a rendere successivamente fraudolento l'utilizzo delle carte stesse. In tale ultima ipotesi emerge in maniera evidente la volontà di anticipare l'intervento penale ad un stadio di pericolo astratto ancora lontano dalla possibilità di lesione concreta del bene giuridico protetto: viene sanzionata una mera situazione di fatto consistente nella disponibilità di una carta (possesso, acquisto o cessione) di provenienza illecita oppure falsificata o alterata, senza che sia necessaria la prova di un concreto pericolo per il bene giuridico protetto o una qualsivoglia lesione allo stesso.

Il dato normativo consta di varie condotte autonomamente rilevanti, risultando difatti possibile isolare l'indebito utilizzo di carte di credito o di pagamento, la falsificazione e l'alterazione delle stesse ed infine il possesso, la cessione o l'acquisto di carte di credito o di pagamento di provenienza illecita o comunque falsificate o alterate. Le Sezioni unite penali della Suprema Corte si sono espresse presto in tal senso[9] sulla scorta dell'interpretazione logica e letterale della norma. La disposizione in esame, dunque, descriverebbe distinte fattispecie criminose ovvero, da un lato, l'indebita utilizzazione di carte di credito (e documenti affini), e, dall'altra, il possesso, la cessione o l'acquisizione di tali documenti di provenienza illecita. Si noti altresì che, stante l'eterogeneità strutturale e temporale delle fattispecie anzidette, è ben possibile che i reati *de quibus* concorrano tra loro[10].

In giurisprudenza, si è sottolineato presto come il verbo "utilizzare" debba

[9] Cass., sez. Unite sent. n. 22902 del 2001, "*Tiezzi*".
[10] Cass. Pen., sez. I, sent. n. 46354 del 5/11/2003.

essere inteso nella sua accezione più ampia, dato che la norma prescinde dalla individuazione di modalità precise della condotta: significa dunque carpire i codici di utenza, rendere utile, mettere a profitto, sfruttare e, nella comune accezione giuridica, indica l'uso del documento corrispondente alla sua destinazione funzionale. Parte della giurisprudenza ha inoltre sostenuto come si debba prescindere dalla necessità che l'agente si trovi in possesso del documento anzidetto: la materiale disponibilità della carta non rappresenta elemento necessario per la configurazione della fattispecie criminosa, ben potendo ritenersi integrato il reato in esame con la realizzazione di transazioni tramite l'inserimento nella rete telematica dei codici (o comunque dei dati) appartenenti ad una carta di credito[11]. Tale ricostruzione avrebbe tuttavia incontrato resistenza da parte di alcuni in dottrina, i quali hanno rilevato come da un lato un simile argomentare finirebbe per condurre ad una applicazione *in malam partem* del dato normativo; dall'altro si arriverebbe a sovrapporre l'ambito applicativo del reato *de quo* a quello della frode informatica, nella quale più propriamente è possibile includere "l'intervento senza diritto" in un sistema informatico o telematico.

Le posizioni tornano ad essere univoche invece relativamente all'individuazione dei confini del concetto di "indebito utilizzo": si ritiene concordemente che l'uso risulti indebito – e dunque penalmente rilevante – allorché in primis questo avvenga da parte di colui che non ne è titolare, ovvero contro la volontà di quest'ultimo, oppure qualora la carta venga usata secondo modalità contrastanti con le norme che ne regolano l'uso.

Sempre per anticipare la soglia della punibilità, tutte le condotte inoltre vengono punite a titolo di dolo specifico: la disposizione richiede espressamente che l'utilizzo, la falsificazione o l'alterazione degli strumenti di pagamento avvengano al preciso fine di trarre profitto per sé o per altri. In altri termini, non è necessario che si verifichi in via di fatto un vantaggio economicamente valutabile conseguente alla condotta fraudolenta, essendo sufficiente che esso

[11] "*Integra il reato l'effettuazione attraverso la rete internet di transazioni, previa immissione dei dati ricognitivi e operativi di una valida carta di credito altrui, acquisiti dall'agente fraudolentemente con il sistema telematico, a nulla rilevando che il documento non sia stato nel suo materiale possesso*", Cass. Pen., sez. I, sent. n. 37115 del 2/10/2002, "*Debernardi*".

rimanga allo stadio di scopo nella psiche dell'agente che comunque possa essere univocamente provato sulla base di elementi di fatto. Tale requisito è fondamentale, poiché è il solo che realmente consente di distinguere i casi nei quali l'agente è mosso da scopi illeciti e quindi merita una sanzione da quelli in cui per le ragioni più diverse, agisce senza la volontà di un profitto illecito[12].

Per la consumazione del reato non è quindi richiesta la lesione effettiva del bene giuridico tutelato e non è altresì necessario che l'agente consegua la materiale disponibilità di un profitto patrimoniale: il reato è da considerarsi integrato ogni qualvolta avvenga l'utilizzo indebito della carta o attraverso l'inserimento della stessa nell'apparecchio di lettura del distributore di banconote o presso gli esercenti convenzionati POS.

La giurisprudenza maggioritaria – anche di legittimità – avvalora tale linea interpretativa, sostenendo che il reato di indebito utilizzo di carte di pagamento si realizzerebbe indipendentemente dal conseguimento da parte dell'agente di qualsivoglia profitto ovvero dal verificarsi di un danno: tali eventi si pongono entrambi quali post-fatti non rilevanti ai fini della punibilità (rilevanti semmai per la determinazione della pena ex art. 133 c.p.)[13]. Deve dunque ritenersi consumato il reato *de quo* allorché un soggetto utilizzi indebitamente carte di credito con il fine specifico di profitto per sé ovvero per altri, e pur tuttavia senza che rilevi l'effettivo conseguimento di suddetto profitto, il quale dunque risulta essere elemento estraneo alla struttura del reato.

Come per tutti i reati di pericolo è complessa nel concreto la configurazione del tentativo, poiché risulta quasi impossibile individuare "*atti idonei, diretti in modo non equivoco*" ex art. 56 c.p. alla commissione di un delitto che non è caratterizzato da una tangibile e misurabile lesione al bene giuridico, bensì sanziona la mera messa in pericolo dello stesso. Il rischio è di anticipare eccessivamente la soglia della punibilità rispetto al canone di ragionevolezza, che sempre deve ispirare l'attuazione del diritto, arrivando a colpire comportamenti che non sono caratterizzati da una reale offensività. Inoltre, per

[12] Ad esempio il caso in cui il titolare della carta la spende senza essersi accorto della sopravvenuta scadenza della stessa.

[13] Cass. Pen., sez. V, sent. n. 44362 del 19/11/2003; Cass. Pen. sez. I, sent. n. 42888 del 26/10/2004.

quanto riguarda la condotta di mero possesso, attraverso la quale si predispone una tutela prodromica anche rispetto ad un utilizzo solo potenziale del documento elettronico, la configurazione del tentativo risulta ancor meno sostenibile, dato che si è molto lontani da un qualsiasi rischio reale per il bene giuridico nonché a maggior ragione da qualsiasi lesione del medesimo. C'è da dire poi che in tali ipotesi sarebbe a rischio anche la tenuta del principio di *extrema ratio* dell'intervento penale; senza contare infine l'estrema difficoltà dal punto di vista della ricerca della prova del dolo specifico in una situazione meramente prodromica ad una successiva situazione di pericolo.

I giudici di legittimità, al fine di individuare dei parametri più certi in base ai quali contestare il delitto consumato ovvero il mero delitto tentato, hanno distinto fra carte il cui uso non richiede la cooperazione dell'utente e carte che possono essere sfruttate solo mediante la digitazione di un p.i.n. o attraverso qualche altro tipo di mezzo di identificazione che richiede la collaborazione del legittimo titolare: nel primo caso, il delitto di indebito utilizzo appare consumato già nel momento in cui il documento elettronico viene consegnato all'esattore per il pagamento del bene o servizio, essendo sufficiente che l'utente attenda il disbrigo delle necessarie registrazioni da parte del medesimo[14]; tale interpretazione viene spiegata dai giudici anche alla luce della natura composita del bene giuridico tutelato dalla fattispecie in commento, *"che attiene non solo ad un ambito patrimoniale squisitamente privato (e, dunque, proprio del titolare della carta di credito e/o del soggetto emittente), ma anche ad una sfera di interessi pubblici, quali l'interesse d'impedire che il sistema finanziario venga utilizzato ai fini di riciclaggio e quello di salvaguardare, al tempo stesso, la fede pubblica".*

Nel diverso caso di necessaria collaborazione da parte del titolare della carta, tutte le volte che la stessa non avrà luogo – per qualsivoglia motivo – il delitto rimarrà allo stadio del tentativo[15] con la conseguenza di ampliare notevolmente

[14] Per es. utilizzo di una carta di pagamento a credito altrui che non richieda un p.i.n. per l'acquisto di beni o servizi: in questo caso il delitto appare non già solo tentato ma perfettamente consumato pure nel caso in cui manchi la materiale apprensione dei beni o servizi per l'acquisto dei quali è stata sfruttata la carta altrui.

[15] Cass. Pen. sez. V, sent. n. 4295 del 24/4/1996, con specifico riferimento alla condotta di chi introduca una carta bancomat di illecita provenienza in uno sportello automatico e, non

la configurabilità dello stesso e di lasciare alla discrezionalità giudiziale l'individuazione del fine e dell'idoneità degli atti[16].

Rispetto alla posizione dei giudici della Suprema Corte, forse sarebbe più corretto escludere dall'alveo del tentativo – e considerare il delitto consumato – nel caso in cui la materiale apprensione delle banconote o del profitto in generale non sia stata resa possibile solamente per l'intervento delle forze dell'ordine: bisogna ricordare la struttura della fattispecie come reato di mera condotta a dolo specifico, dunque se l'unico evento interruttivo risulta essere la pronta azione delle forze di polizia e vi è già stata la cooperazione dell'utente per accedere al servizio, risulta che nulla manca per la configurazione del fatto di reato in tutti i suoi elementi tipici.

Fin dalla sua introduzione nel 1991, la disciplina penale delle carte di credito o di pagamento ha suscitato un vivace ed intenso dibattito relativamente alla questione dei rapporti con le fattispecie "limitrofe", vale a dire in un primo momento solo la truffa (art. 640 c.p.) e successivamente anche la frode informatica di cui all'art. 640-ter c.p.

Volgendo lo sguardo al rapporto con il delitto di truffa, si osserva come questo ricorra allorché l'agente procuri un ingiusto profitto con danno altrui per sé o per altri, ponendo in essere "*artifizi e raggiri*" tali da determinare in altri un errore. La giurisprudenza si è in particolare soffermata sui concetti di "artifizio" e "raggiro", in quanto elementi caratterizzanti la condotta dell'agente e li ha interpretati, dopo diverse oscillazioni, in maniera piuttosto lata, ricomprendendo al loro interno condotte sia attive che omissive, sia false rappresentazioni della realtà sia semplici menzogne. Ciò che effettivamente rileva non sono dunque le modalità operative concretamente poste in essere, quanto piuttosto l'idoneità della condotta ad indurre altri in errore, ovvero a rafforzare o comunque avvalorare una pregressa errata rappresentazione dei fatti in un altro soggetto[17]. *Punctum dolens* è dunque stabilire se l'uso indebito di carte di

---

disponendo del codice di accesso, esegua una serie di combinazioni numeriche al fine di conseguire il danaro, senza riuscirvi.

[16] Cass. Pen., sez. V, sent. n. 23429 del 08/06/2001; in tal senso anche Cass. Pen., sez. I, sent. n. 2409 del 28/4/1998.

[17] Dato che l'art. 640 c.p. risulta esser posto a presidio, come rilevato da alcune pronunce, non solo del patrimonio, ma altresì della libertà della prestazione del consenso nelle transazioni.

credito o di pagamento possa configurarsi come specificazione degli artifizi e raggiri di cui all'art. 640 c.p.[18], poiché risulta astrattamente sussumibile sotto entrambe le disposizioni suindicate la condotta di colui il quale, utilizzando "indebitamente" una carta di credito o di pagamento, proceda, ad esempio, all'acquisto di un certo bene ricavandone un vantaggio. Rimane ferma la configurazione del delitto di truffa nel caso in cui lo spostamento patrimoniale sia posto in essere dal soggetto passivo sulla base di un induzione in errore causata dalla condotta fraudolenta dell'agente.

Invero, la giurisprudenza è stata a lungo divisa, affermando talora il concorso di reati e talaltra il concorso apparente di norme. Secondo un primo orientamento, affermatosi in vigenza della legge n. 143 del 1991, tra il reato ex art. 640 c.p. e quello ex art. 12 l. cit. prima parte vi sarebbe stato concorso di reati, a seconda dei casi materiale o formale. Tale conclusione si fondava anzitutto sul rilievo formale per cui le due fattispecie in esame erano state introdotte dal legislatore a presidio di diversi beni giuridici: nel caso della truffa si trattava del patrimonio del privato; nel caso di indebito utilizzo invece il presidio aveva natura eminentemente pubblicistica, stante l'interesse ad evitare che il sistema finanziario venga utilizzato per riciclare denaro "sporco" (mentre la tutela del patrimonio dei privati riceve tutela solo indiretta). Veniva inoltre sottolineata la diversità strutturale tra le due fattispecie, in quanto la truffa, contrariamente alla fattispecie di indebito utilizzo, è un delitto a bilateralità necessaria e richiede per la propria configurabilità il verificarsi dell'evento (conseguimento di un profitto ed il verificarsi di un danno). Perciò fra le due fattispecie incriminatrici non poteva sussistere un rapporto di specialità: doveva essere escluso il concorso apparente di norme e, al contrario, si affermava il concorso di reati, formale o materiale a seconda della condotta tenuta dall'agente nel caso concreto.

A tale impostazione si contrapponeva altro orientamento giurisprudenziale, il quale invece affermava la configurabilità nel caso di specie di un concorso apparente di norme, da risolvere alla luce del criterio di specialità fissato dall'art. 15 c.p. In particolare, si sosteneva che non era possibile configurare un

[18] La disposizione extra codicistica prevede tre autonome condotte: i problemi di coordinamento sono sorti con la prima fattispecie prevista, l'indebito utilizzo dello strumento di pagamento, stante la totale eterogeneità strutturale delle altre due condotte rispetto alla truffa.

concorso di reati, essendo anche il reato di indebito utilizzo di carte di credito volto a tutelare in una certa misura il patrimonio del privato. Inoltre le fattispecie presentavano dei contenuti reciprocamente speciali, venendo in diverso modo specificate le condotte aventi rilevanza penale e nell'art. 12 l. cit. altresì l'oggetto materiale sul quale debbono ricadere[19].

L'ampiezza della sfera di applicabilità e la struttura normativa di reato di mera condotta la rendevano un efficace presidio autonomo: poteva ben ricomprendere tanto le ipotesi in cui il danno si fosse verificato (come per la truffa) quanto quelle in cui invece ancora mancasse. Conseguentemente veniva a crearsi un rapporto di genere-specie, da risolvere ex art. 15 c.p. con la prevalenza della fattispecie speciale più grave, l'art. 12 della legge del 1991.

Tale contrasto giurisprudenziale è stato infine risolto dalla sentenza delle SS. UU. "*Tiezzi*" del 2001, la quale ha ritenuto di aderire all'orientamento da ultimo richiamato, seppur diversamente motivando; successivamente altre pronunce di Cassazione del 2005 hanno confermato tale opzione interpretativa.

I giudici di legittimità hanno argomentato l'assenza di concorso di reati partendo dall'analisi delle condotte fraudolente e sottolineando come in realtà "*non si è in presenza di due fatti completamente distinti dalla materialità della condotta, poiché appare evidente che l'adozione di artifizi o raggiri è uno dei possibili modi in cui si estrinseca l'uso indebito di una carta di credito, sicché la prima di tali condotte ben può identificarsi nella seconda come specie a genere*". Successivamente l'analisi si sofferma sulle obiettività giuridiche: la norma di cui all'art. 12 non è posta a tutela esclusiva di un interesse di natura pubblicistica, tutelando anch'essa il patrimonio del privato posto in pericolo a causa dell'indebito utilizzo di strumenti di pagamento elettronico[20].

Nemmeno il profitto e il danno richiesti dall'art. 640 c.p. possono essere utilizzati per affermare la diversità dei fatti: si tratta di dati fattuali che "*non possono trasformare una tale situazione di identità ontologica dell'azione in totale diversità del fatto*", configurandosi come fattori specializzanti rispetto

[19] Anche C. Cuomo – R. Razzante, *op.cit.* concordano con questo orientamento, ritenendo che l'adozione di artifici e raggiri è uno dei possibili modi in cui può avvenire l'uso indebito della carta di pagamento.

[20] Vedi cap. II par. 1

all'art. 12 l. cit.

Le due norme si pongono in rapporto di specialità bilaterale: ognuna è caratterizzata da fattori specializzanti rispetto all'altra, perciò è necessario individuare un criterio in base al quale stabilire quale prevalga nel caso concreto. Essendo il principio di specialità ex art. 15 c.p. di difficile applicazione sia in astratto sia in concreto[21], i giudici optano per l'applicazione del criterio dell'assorbimento, "*parametro di valore sotteso all'intero sistema e probabilmente recepibile in forma espressa dal legislatore futuro*".

Viene così affermato il concorso apparente di norme tra le due fattispecie in esame: l'art. 12 l. cit. prevede infatti una pena ben più grave rispetto a quella prevista dalla norma codicistica e ne esaurisce la carica offensiva, anche grazie all'anticipazione della soglia della punibilità alla mera condotta fraudolenta finalizzata al conseguimento del profitto. Ragion per cui deve ritenersi che la prima fattispecie esaurisca il disvalore giuridico anche della seconda[22].

Più recentemente, la Cassazione, in accordo con i giudici di merito, ha avuto modo di sottolineare come non sia in assoluto esclusa la possibilità di concorso tra la truffa e l'indebito utilizzo di strumenti di pagamento: è configurabile il concorso ogni qualvolta gli artifizi o raggiri non si sostanzino ed esauriscano l'indebito utilizzo, bensì vi sia un *quid pluris* fraudolento nella condotta dell'agente che si affianca all'utilizzo fraudolento dello strumento di pagamento[23].

Con l'introduzione dell'art. 640-ter c.p. è risultata molto controversa anche la questione dei rapporti tra il reato codicistico di frode informatica e la

---

[21] I motivi sono fondamentalmente due: in primis, l'ardua perimetrazione del concetto di "stessa materia", che è presupposto applicativo dell'art. 15 c.p.; in secundis, l'incapacità del criterio di specialità di definire i rapporti tra certe categorie di norme, rispetto alle quali risulta impossibile individuare quale tra esse sia la norma speciale (e dunque applicabile) e quale la generale.

[22] La giurisprudenza è concorde nel ritenere che il principio di assorbimento può operare solo in presenza di due condizioni: la norma assorbente esaurisca il disvalore della norma assorbita e preveda altresì un trattamento sanzionatorio più grave. Quest'ultimo infatti mostrerebbe inequivocabilmente la *voluntas legis* di considerare le due disposizioni penali come un *unicum* ai fini della pena.

[23] Cass. Pen., Sez. Fer., sent. n. 45946 del 15/09/2011-12/12/2011: "*il reato di truffa non è assorbito in quello di indebita utilizzazione, a fine di profitto proprio o altrui, da parte di chi non ne sia titolare, di carte di credito o analoghi strumenti di prelievo o pagamento, se la condotta incriminata non si esaurisca nel mero utilizzo del documento predetto ma sia connotata, come nel caso in esame, da un quid pluris, ossia dall'artifizio consistente nel carpire ed utilizzare, invito domino, il codice alfanumerico*". Nelle intenzioni dei clienti, intatti, quest'ultimo doveva restare segreto fino alla consegna della merce, oggetto della transazione commerciale.

disposizione in esame. Mentre per la terza fattispecie prevista all'art. 55 – possesso, cessione, acquisizione di documenti di pagamento di provenienza illecita – non si ravvisano particolari interferenze rispetto alla frode informatica con cui v'è concorso materiale di reati, la questione dei rapporti tra gli altri due commi e la norma codicistica deriva dal fatto che l'art. 55 c. IX attiene non solo alle carte di credito o di pagamento tradizionali, ma anche a qualsiasi "*documento analogo*", categoria in cui rientrano pacificamente le carte magnetiche, sui cui sono impressi "dati pertinenti ad un sistema informatico" e le recenti carte a *microchip*, che costituiscono un vero e proprio autonomo sistema informatico. Perciò risulta necessario riuscire ad armonizzare la disciplina nel caso in cui si verifichi l'utilizzo abusivo di una carta magnetica, con profitto ingiusto ed altrui danno senza che occorrano atti di disposizione di una persona indotta in errore.

L'analisi si incentra sulle condotte tipizzate: laddove la condotta si sostanzi nella mera utilizzazione indebita di carte di credito o di pagamento magnetiche da parte di persona non legittimata, senza manipolazioni dei dati, non può configurarsi la frode informatica, poiché manca totalmente la condotta tipica, sia essa alterativa o manipolativa, che abbia come oggetto immediato un sistema informatico o telematico. Laddove, viceversa, l'azione fraudolenta posta in essere concerna la falsificazione o l'alterazione di una carta di credito o di pagamento (o di qualsiasi altro documento analogo) attraverso una manipolazione dei dati presenti nel supporto di memoria magnetica o conservati nel *microchip* della carta potrebbe configurare un concorso di reati[24].

La dottrina sarebbe per lo più orientata nel senso di escludere detto concorso di reati, ritenendo che vada applicata la norma più grave di cui alla normativa Antiriciclaggio, assorbente rispetto all'art. 640-ter c.p.: l'iter argomentativo segue da vicino quello che è stato utilizzato per escludere il concorso fra la norma extra codicistica e la fattispecie di truffa tradizionale, basandosi sulla prevalenza della fattispecie più grave, in grado di esaurire la carica offensiva

[24] Il caso classico è quello dell'utilizzo di uno *skimmer*, cioè di un lettore di carte di credito o debito che viene fraudolentemente applicato sopra l'apparecchio automatico di tipo bancomat, in modo tale da non venire riconosciuto dall'ignaro utente. È progettato per captare i dati delle altrui autentiche carte di credito, da usare poi per falsificarne o eseguire operazioni sulle stesse ai danni del legittimo titolare.

della condotta, nel caso di più fattispecie poste a tutela dello stesso bene giuridico.

La giurisprudenza, dal canto suo, è stata generalmente divisa rispetto alla possibilità di concorso di reati, ritenendo una parte che il concorso di reati fosse da escludere dato che le due fattispecie sono poste a tutela del medesimo bene giuridico e ognuna possiede il proprio ambito applicativo, un'altra parte invece sostenendo che le due norme possono pacificamente concorrere stante il rapporto di specialità bilaterale che le caratterizza e la diversità di bene giuridico tutelato. Invero, anche fra coloro che non ritengono configurabile il concorso di reati si registrano divergenze d'opinione rispetto alla scelta di quale norma debba prevalere. Sembra comunque che la giurisprudenza maggioritaria sia alla ricerca di un criterio dirimente che permetta alla due fattispecie di convivere, avendo ognuna un autonomo ambito applicativo.

Si è così ritenuto che debba prevalere il delitto di frode informatica nel "*fatto di colui che, servendosi di una carta di credito falsificata e di un codice di accesso fraudolentemente captato in precedenza, penetri abusivamente nel sistema informatico bancario ed effettui illecite operazioni di trasferimento fondi, tra cui quella di prelievo di contanti attraverso i servizi di cassa continua*"[25].

Recentemente sia pronunce di merito sia pronunce di legittimità hanno espressamente ribadito questo principio, individuando la frode informatica in quei casi nei quali la carta di pagamento non viene usata in quanto tale ma funge solo da grimaldello per porre in essere una condotta manipolativa del sistema informatico o telematico ovvero per intervenire senza legittimazione sullo stesso, effettuando movimenti patrimoniali all'insaputa del titolare[26].

La condotta dirimente risulta la penetrazione abusiva nel sistema informatico bancario cui succede l'effettuazione di operazioni di bonifico, accredito o altri ordini, procurandosi un ingiusto profitto con pari danno per il titolare del conto oggetto degli interventi. L'utilizzazione fraudolenta del sistema informatico, costituisce elemento specializzante nonché presupposto "assorbente" rispetto

[25] Cass. Pen., sez. II, sent. n. 17748 del 15/04/2011 di rigetto del ricorso avverso la sentenza resa il 09/07/2010 dalla Corte d'Appello di Bologna.
[26] Cass. Pen., sez. II, sent. n. 11699 del 10/01-28/03/2012.

alla generica indebita utilizzazione di una carta di credito[27].

Molto interessante è il tentativo di portare chiarezza nel panorama applicativo effettuato dal Tribunale di Monza con due sentenze emesse a pochissima distanza l'una dall'altra.

In entrambi i casi le persone offese erano state vittime del c.d. *Phishing*: erano state tratte in errore mediante una mail, in apparenza proveniente da Poste Italiane, che le invitava a fornire i codici di utilizzo delle loro carte; in realtà tali dati venivano poi strumentalmente utilizzati dagli autori del fatto per effettuare disposizioni di pagamento in proprio favore.

La Procura della Repubblica aveva avanzato in entrambi i casi la più grave contestazione della legge antiriciclaggio; il Tribunale, invece, accogliendo la tesi interpretativa della recente pronuncia di legittimità sopra citata[28] riqualificava i reati nella meno grave ipotesi di frode informatica.

Il giudice individua la distinzione tra i suddetti delitti nella condotta materiale posta in essere dagli autori del fatto: nel caso di frode informatica il soggetto attivo del reato non entra mai in possesso fisicamente della carta di credito ma ne carpisce soltanto i codici di accesso mediante, come nel caso di specie, una mail ingannatrice. Diversamente, il reato di utilizzazione indebita si realizza attraverso l'apprensione fisica della carta da parte di soggetto non autorizzato, che la utilizza per proprie finalità senza alcuna forma di manipolazione, a tal punto che parte della dottrina si è chiesta se detto reato possa concorrere con quello di furto con mezzi fraudolenti.

La tesi della giurisprudenza di legittimità fatta propria dal Tribunale di Monza appare convincente nell'individuare gli elementi distintivi fra le due diverse ipotesi criminose: nell'utilizzazione indebita, l'attenzione si sofferma sulle caratteristiche della carta abilitante al prelievo o al pagamento e fulcro della condotta diventa l'utilizzo della stessa come "denaro elettronico" sostitutiva del contante. La frode informatica invece si rinviene in tutti quei casi nei quali la carta non è utilizzata per le sue precipue finalità, ma è un mezzo che abilita ad operare su un sistema informatico o telematico e in questo modo ottenere un

[27] Tribunale di Napoli, G.U.P. Gallo, sent. n. 1653 del 4/07/2013.
[28] Vedi nota 25

profitto: si potrebbe ipotizzare un concorso fra queste due norme solo allorquando la condotta di utilizzo indebito sia preceduta da un'opera di captazione di segni, simboli e scritte- una vera e propria falsificazione o alterazione di una carta di credito o di pagamento- ottenuta mediante manipolazione dei dati informatici.

4.2. Frode informatica e accesso abusivo al sistema informatico e telematico

La Corte di Cassazione già da tempo ammette il concorso tra il delitto di accesso abusivo ad un sistema informatico di cui all'art. 615-ter c.p. e la frode informatica, dato che, per usare le parole della stessa Corte, "*trattasi di reati totalmente diversi, il secondo dei quali postula necessariamente la manipolazione del sistema, elemento costitutivo non necessario per la consumazione del primo: la differenza fra le due ipotesi criminose si ricava, inoltre, dalla diversità dei beni giuridici tutelati, dall'elemento soggettivo e dalla previsione della possibilità di commettere il reato di accesso abusivo solo nei riguardi di sistemi protetti, caratteristica che non ricorre nel reato di frode informatica*"[29].

Il dettato normativo dell'art. 615-ter c.p. così recita "*Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione sino a tre anni*. […][30]."

[29] Cass. Pen., sez. VI, sent. n. 3067 del 4/10/1999, *Piersanti*, ripresa in Cass. Pen., sez. V, sent. n. 2672 del 27/01/2004 (ud. 1/10/2004), Cass. Pen., sez. V, sent. n. 1727 del 30/09/2008.

[30] La disposizione così prosegue: "*la pena è della reclusione da uno a cinque anni: 1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di pubblico servizio, con abuso dei poteri, o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o abuso della qualità di operatore del sistema; 2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato; 3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti. Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede a querela della persona offesa*".

Il progresso tecnologico ha determinato l'emersione di una vera e propria realtà virtuale (*Cyberspace*) nella quale si sono creati luoghi ulteriori rispetto a quelli tradizionali attentamente protetti dall'ordinamento, dove il soggetto esplica la propria personalità e coltiva i propri interessi. Il luogo informatico nasce dall'immissione di dati in un sistema informatico o telematico ed acquista una entità propria che lo separa dall'esterno con l'ausilio di altre informazioni, quali ad esempio le chiavi logiche di accesso al sistema.

Per proteggere queste particolari realtà, è stata introdotta la fattispecie di accesso abusivo ad un sistema informatico o telematico, la quale risulta dunque caratterizzata da un oggetto giuridico differente rispetto a quello che trova presidio nella frode informatica: si tratta del c.d. *domicilio informatico*, proiezione virtuale del domicilio tutelato ex art. 14 Cost., tutelato sotto il profilo dello "*ius excludendi alios*" nonché in relazione alle modalità che regolano l'accesso di soggetti eventualmente abilitati[31] e connesso al rispetto della privacy individuale, che deve sempre essere preservata dalle moderne forme di aggressione e di interferenza.

Si tratta di un reato di mera condotta, che si consuma nel momento stesso dell'introduzione indebita e la conseguente violazione delle misure di sicurezza predisposte dal titolare del sistema: l'accesso ha carattere "elettronico" o "telematico", poiché può essere realizzato unicamente attraverso le apparecchiature che costituiscono le consuete modalità di ingresso al sistema informatico o telematico e che consentono di interagire con i dati ed i programmi ivi contenuti. È inoltre prevista una seconda modalità della condotta fraudolenta, ravvisabile nell'azione del soggetto abilitato all'accesso che si introduca legittimamente nel sistema ma vi si mantenga poi in maniera indebita, con tempistiche o per finalità diverse da quelle delimitate specificamente dalla sua funzione e dagli scopi per i quali le credenziali d'accesso gli sono state assegnate.

Pur non ravvisandosi un rapporto di specialità tecnica tra le due norme che attengono a fatti materiali diversi, potrebbe sussistere una correlazione tra le due figure, nelle ipotesi in cui la condotta fraudolenta sia posta in essere da

[31] Cass. Pen., sez. V, sent. n. 1727 del 30/09/2008.

persona non abilitata o “da lontano” per via telematica, forzando le misure di sicurezza imposte dal legittimo utente. Spesso l'accesso abusivo non esaurisce la propria funzione in sé stesso, bensì è volto a commettere la frode e, pertanto, ne costituisce una modalità necessaria e prodromica[32].

La prodromicità logica e materiale dell'azione di accesso abusivo non fa escludere la possibilità di un concorso tra le due figure di reato. Infatti l'azione di accesso abusivo non rientra nello schema tipico della frode informatica, che si basa sulla manipolazione del sistema e che quindi può ben consumarsi indipendentemente da esso. Le due fattispecie incriminano fatti materiali differenti che, tuttavia, dal punto di vista fenomenologico possono riscontrarsi contestualmente: non si tratta di fattispecie di cui una inglobi strutturalmente l'altra. Stante quindi la diversità di bene giuridico tutelato e la diversità di condotta incriminata appare ipotizzabile il concorso di reati.

Il concorso può manifestarsi come concorso formale o come concorso materiale: il primo si avrà nel caso in cui l’azione di accesso abusivo rechi già in sé la manipolazione del software necessaria per ottenere l'indebito profitto, ovvero quando l'unicità dell'azione sia data dal compimento di operazioni in connessione logica, anche se non contestuali. Quando invece la frode è realizzata con diversi accessi e successive operazioni correlate ma distanti nel tempo sussisterà il concorso materiale. Essendo probabilmente ravvisabile il medesimo disegno criminoso, la pluralità di reati confluirà logicamente nel reato continuato (art. 81 c.p.)[33].

Pertanto, nei casi in cui l'accesso abusivo vada a buon fine ma la frode non sia commessa per l’intervento di un fattore esterno a bloccarla, è configurabile il concorso tra il reato di accesso abusivo ed il tentativo di frode informatica. Allo stesso modo, sarà configurabile il concorso nella forma della continuazione, nei casi in cui l'accesso riesca e, grazie ad esso, anche la frode informatica. Nel caso in cui nemmeno l’accesso abusivo arrivi a compimento, l’eventuale finalità di frode sarà penalmente irrilevante: sarà punibile solo il tentativo di accesso abusivo al sistema, ex art. 615-ter c.p. in combinato disposto con l’art. 56 c.p.

[32] C. Del Re, *op.cit.*, p. 88-89.
[33] G. Pica, *op.cit.*, p. 159.

Capitolo V: Problematiche applicative

5.1. La "simmetria ritrovata" delle competenze nella frode informatica e le peculiarità rispetto alle fattispecie limitrofe

Con particolare riguardo all'autorità giudiziaria territorialmente competente, il delitto di frode informatica ha subito una rilevante modifica con la legge n. 48 di ratifica della Convenzione *Cybercrime* del marzo 2008: mentre prima la competenza seguiva le ordinarie regole previste dal codice di procedura penale, con la legge n. 48/2008 si è deciso di far convergere le attività d'indagine per i reati informatici presso la Procura Distrettuale, integrando l'art. 51 c.p.p. con un nuovo c. 3-*quinquies*[1]. Nelle intenzioni del legislatore, la scelta di concentrare a livello distrettuale le indagini sui reati informatici si basava sul riconoscimento della loro specificità e mirava a superare problemi di efficienza nell'attività di contrasto a tale fenomeno criminoso che risulta caratterizzato da un elevato grado di specializzazione tecnica, oltre ad essere difficilmente circoscrivibile entro limitati orizzonti spaziali.

Tale opzione non è stata accolta con favore da tutti in dottrina: alcuni Autori[2] hanno sottolineato il pericolo di appesantire ulteriormente senza una reale necessità il carico di lavoro degli uffici centrali, data l'enorme quantità di notizie di reato in materia di reati informatici e, in particolare, relative alla frode informatica; inoltre si riteneva potesse risultare rischioso incentivare la preparazione specialistica tecnico-informatica solamente in capo ai nuclei investigativi afferenti alla Procure Distrettuali, quando è ormai riconosciuta l'importanza delle competenze informatiche in ogni tipo di indagini. I problemi

[1] Si veda l'art. 11 *(Competenza) l. 48/2008:* "*All'articolo 51 del codice di procedura penale è aggiunto, in fine, il seguente comma: 3-quinquies. Quando si tratta di procedimenti per i delitti, consumati o tentati, di cui agli articoli 600-bis, 600-ter, 600-quater, 600-quater.1, 600-quinquies, 615-ter, 615-quater, 615-quinquies, 617-bis, 617-ter, 617-quater, 617-quinquies, 617-sexies, 635-bis, 635-ter, 635-quater, 640-ter e 640-quinquies del codice penale, le funzioni indicate nel comma 1, lettera a), del presente articolo sono attribuite all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente*".

[2] L. Luparia, "*I correttivi alle distorsioni sistematiche*", in "*Le nuove norme sulla sicurezza pubblica*" di S. Lorusso, Cedam, 2008.

erano anche di tipo prettamente organizzativo: la maggior parte delle neonate "Procure informatiche distrettuali" infatti non avevano, al momento della introduzione della legge n. 48/2008, magistrati già dediti a lavorare come *pool* nelle materie attinenti la cybercriminalità e quindi si sono dovute organizzare *ex novo*, con costi e difficoltà notevoli[3]. Senza contare che alcune procure, come quella di Milano, avevano dato vita ben prima dell'innovazione legislativa del 2008 ad una squadra di magistrati specializzati in delitti informatici[4].

Non è stata prevista nemmeno un'organizzazione strutturata interna fra le varie Procure informatiche, con organi di raccordo simili alla DNA, DDA o alla DIA che permettano un lavoro sinergico e lo sviluppo di modalità investigative comuni: è evidente come ciò osti allo sviluppo di una vera e propria rete nazionale dedicata a tali fenomeni. Forse il legislatore non ha riflettuto a sufficienza sulle possibili conseguenze di una scelta non ben armonizzata nel sistema: anziché incentivare l'efficienza potrebbe portare ad una effettiva paralisi dell'azione penale[5].

Altra ragione a sostegno della tesi critica rispetto alla scelta del legislatore discende da un'osservazione di più ampio respiro che prende a riferimento la *ratio* delle precedenti deroghe ai criteri di devoluzione delle funzioni di pubblico ministero: queste trovavano la loro ragion d'essere nell'unitarietà del fenomeno criminale da contrastare, caratterizzato nel caso dell'organizzazione mafiosa o terroristica da un'estesa e coordinata rete strutturata e articolata sul territorio che richiedeva una risposta giudiziaria univoca, altrettanto coordinata e non parcellizzata fra le singole procure. Nell'ipotesi in esame non è tanto il carattere associativo a venire in rilievo – anche perché in tal caso si sarebbe potuto comunque applicare l'art. 51 c.p.p. attraverso la devoluzione alle Procure Distrettuali di altre fattispecie – quanto la natura specialistica delle indagini

[3] F. Cajani, D. D'Agostino, W. Vannini, "*Di necessità, virtù: appunti per una strategia globale al contrasto del cybercrime. L'esperienza del pool dei reati informatici della Procura di Milano*", in "*IISFA Memberbook 2011 DIGITAL FORENSICS, Condivisione della conoscenza tra i membri dell'IISFA ITALIAN CHAPTER*", Experta, Forlì.

[4] Già dal 2004 la procura di Milano aveva sviluppato all'interno dell'VIII dipartimento una squadra specializzata nell'investigazione informatica, denominata pool reati informatici.

[5] C. Maioli, E. Sanguedolce, "*I "nuovi" mezzi di ricerca della prova fra informatica forense e L. 48/2008*", articolo del 07/05/2012 reperibile su Altalex al seguente link: http://www.altalex.com/documents/altalex/news/2012/05/03/i-nuovi-mezzi-di-ricerca-della-prova-fra-informatica-forense-e-l-48-2008

riguardanti i reati a matrice tecnologica: dunque è lecito chiedersi se tale condizione possa legittimare la deroga, nell'ambito delle indagini preliminari, sia ai fondamentali canoni di ripartizione della competenza per territorio sia al canone costituzionale del "giudice naturale precostituito", con conseguente pregiudizio del diritto di difesa dell'indagato. Inoltre per questa via si profila il rischio di legittimare pro futuro nuovi scostamenti dalle regole ordinarie solamente in ragione della supposta elevata specializzazione dell'uno o l'altro settore d'indagine.

Alcuni hanno poi rilevato come mancava e manchi tuttora, parallelamente alla specializzazione informatica delle Procure Distrettuali, un'azione legislativa volta ad elevare il livello di conoscenza tecnica delle forze di Polizia Giudiziaria presenti sui territori e/o il livello di dotazioni informatiche in uso alle stesse, ancora di gran lunga obsolete per un adeguato contrasto alla criminalità[6].

Comunque non mancavano coloro che rilevavano i pregi del *novum* legislativo: dal punto di vista della politica del diritto avrebbe avuto il merito di contribuire a creare dei *pool* di magistrati con competenze tecniche specialistiche rispetto all'indagine sui *computer crimes* e avrebbe permesso di evitare gli inconvenienti derivanti dalla parcellizzazione dell'azione investigativa su reati che presentano elevati profili di complessità e capillarità.

Cionondimeno, vi era un aspetto sul quale dottrina e giurisprudenza erano pressoché unanimi nel riconoscere una profonda criticità nell'intervento legislativo del 2008, vale a dire la mancata previsione, nell'originaria formulazione, di un esplicito ampliamento della portata applicativa dell'art. 328 c.p.p, tale da spostare a livello distrettuale, per gli stessi reati, la competenza dell'organo giudicante della fase preliminare (G.I.P. e G.U.P.).

Il legislatore aveva sì operato uno spostamento dell'attività investigativa a livello distrettuale, ma aveva omesso di integrare l'art. 328 c.p.p., lasciando che le funzioni giudicanti rimassero di competenza dell'organo del circondario. Tale inusuale scelta finiva per creare una frattura nell'ordinaria simmetria tra regole di competenza territoriale del giudice e criteri di attribuzione delle funzioni di pubblico ministero. Non solo: la mancanza di accentramento a livello

[6] F. Cajani, D. D'Agostino, W. Vannini, *op.cit*.

distrettuale della competenza giudicante avrebbe creato problemi di lungaggini e difficoltà di rapporto fra le parti ed il giudice del procedimento, organo che ha la precipua funzione di tutelare i diritti dell'indagato e degli altri soggetti coinvolti, dal momento che conseguentemente sarebbe sorto l'obbligo di far transitare il procedimento sui *computer crimes* dall'ufficio del P.M. presso la Procura Distrettuale ai giudici territorialmente competenti. Tale aggrovigliata situazione contraddiceva manifestamente sia il principio generale della ragionevole durata del processo sia la stessa *ratio* della novella dell'art. 51 c.p.p. di creare *pool* di magistrati specializzati in reati informatici, poiché si attribuiva a giudici senza alcuna esperienza in materia di criminalità informatica il compito di valutare l'operato di un pubblico ministero munito di una specifica preparazione. Tale eventualità non sarebbe stata in linea con la filosofia che è all'origine del diverso sistema organizzativo e avrebbe determinato costi certamente superiori rispetto ai vantaggi derivanti dall'introduzione di una attribuzione investigativa specialistica. Senza contare gli inconvenienti anche sul piano più strettamente procedimentale, poiché dalla mancanza di simmetria fra competenza territoriale e attribuzioni al P.M. derivava un considerevole ampliamento delle ipotesi di conflitto fra uffici giudiziari: infatti, stante un simile riparto delle competenze, l'eventualità di un provvedimento giurisdizionale nel quale fosse dichiarata l'incompetenza del G.I.P. avrebbe avuto conseguenze pregiudizievoli non di poco conto.

Fortunatamente il legislatore ordinario è intervenuto a porre rimedio a tale svista, con la conversione del D.L. n. 92 del 23 maggio 2008, recante misure urgenti in materia di sicurezza pubblica, nella legge n. 125 del 24 luglio 2008. L'art. 2, c. 1, lett. *a)* ha aggiunto il comma 1-*quater all'art. 328 c.p.p.*, a norma del quale "*quando si tratta di procedimenti per i delitti indicati nell'art. 51, comma 3-quinquies, le funzioni di giudice per le indagini preliminari e le funzioni di giudice per l'udienza preliminare sono esercitate, salve specifiche disposizioni di legge, da un magistrato del tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente*".

Il quadro che ne risulta, pertanto, appare finalmente dotato di una coerenza interna, anche se permangono dubbi circa l'opportunità di una simile deroga.

L'intervento del legislatore è apparso fin da subito necessario, poiché si stavano affacciando in giurisprudenza orientamenti interpretativi che denotavano una certa confusione relativamente all'affermazione o al diniego di competenza. In particolare, degna di nota è stata la sentenza di Cassazione n. 45078 depositata il 4 dicembre 2008, con cui il giudice delle leggi è stato chiamato a risolvere un conflitto negativo di competenza sollevato dal G.I.P. del Tribunale di Napoli avverso il provvedimento con cui il G.I.P. del Tribunale di Nola dichiarava la propria incompetenza sui delitti di cui all'art. 640-*ter* c.p., benché commessi nell'ambito della propria competenza territoriale. Il G.I.P. del Tribunale di Nola aveva motivato la propria declaratoria di incompetenza proprio facendo riferimento alla recente modificazione delle attribuzioni degli uffici del Pubblico Ministero introdotta con la l. 48/2008, che ha comportato, relativamente ai *computer crimes*, lo spostamento delle indagini in capo ai P.M. della Procura Distrettuale.

Rilevando come la legge di ratifica della Convenzione *Cybercrime* non avesse apportato alcuna modifica all'art. 328 c.p.p. e determinandosi quindi un difetto di coordinamento, il G.I.P. di Nola ha ritenuto che si dovesse risolvere tale situazione a livello ermeneutico, desumendo dall'attribuzione della competenza al P.M. del capoluogo del distretto un implicito conferimento di competenza al giudice per le indagini preliminari dello stesso tribunale. Ciò sulla base di un principio implicito nel sistema, in base al quale il giudice per le indagini preliminari è sempre quello presso il quale si trova il P.M. competente.

Il G.I.P. del Tribunale di Napoli si opponeva a tale provvedimento e sollevava conflitto negativo di competenza innanzi alla Corte di Cassazione, contestando *in toto* l'argomentazione dell'organo giudicante del Tribunale territoriale, sulla base di un'interpretazione più formalistica e sistematica dei dati normativi. In assenza di un'esplicita previsione sull'intervento del giudice nel procedimento, la competenza si determina sulla base delle regole ordinarie previste dal codice di procedura penale: non è ammissibile ricavare una competenza derogatoria interpretando un supposto principio generale implicito nell'ordinamento, come tale troppo volatile e incerto, pena la violazione dell'art. 25 Cost. e il principio del giudice naturale precostituito per legge. Inoltre, se si vuole far riferimento a

principi guida del sistema processuale penale, dottrina e giurisprudenza sono concordi nel ritenere che in linea generale sia il pubblico ministero a trarre la propria legittimazione in maniera derivata rispetto a quella del giudice[7], non il contrario. Quella del legislatore era da considerare a tutti gli effetti una scelta di politica legislativa, non sconfessabile a livello operativo: ne era dimostrazione la circostanza che, ogniqualvolta si era proceduto a novellare l'art. 51 c.p.p. al fine di trasferire le attribuzioni del pubblico ministero a livello distrettuale, il legislatore contestualmente aveva sempre operato una modifica dell'art. 328 c.p.p. al fine di modificare anche la competenza del giudice.

La Corte di Cassazione ha accolto senza riserve l'impostazione proposta dal G.I.P. del Tribunale di Napoli, ritenendo applicabili ai fini della determinazione della competenza gli ordinari criteri di ripartizione previsti dal codice di procedura penale, pur a seguito dell'ampliamento delle attribuzioni del pubblico ministero distrettuale. L'argomentazione dei giudici di legittimità è risultata più agevole anche grazie all'intervento correttivo del legislatore del luglio 2008, che ha introdotto la competenza distrettuale altresì dell'organo giudicante[8]. Comunque, in mancanza di apposita previsione legislativa, il G.I.P. non può ricavare dalle disposizioni sulla attribuzione di funzioni del pubblico ministero un fondamento per legittimare una competenza non espressamente attribuitagli dalla legge: ove il G.I.P. del tribunale del capoluogo avesse emanato un provvedimento fuori dalle tassative ipotesi di competenza distrettuale disegnate dall'art. 328, c. 1-*bis* c.p.p., sostituendosi al G.I.P. del tribunale territorialmente competente in relazione al luogo di commissione del reato, tale provvedimento sarebbe risultato viziato per incompetenza territoriale.

Probabilmente la Cassazione, pur prefigurandosi scenari di seria complessità, in assenza dell'opportuna correzione legislativa non avrebbe potuto optare per una diversa ricostruzione dell'impianto normativo prodotto dalla legge n. 48,

[7] Ordinariamente, infatti, le attribuzioni del P.M. sono derivate e serventi rispetto alla disciplina della competenza del giudice, nel senso che esse si modellano e si delimitano in esatta corrispondenza alle regole di ripartizione della competenza tra giudici di cui agli artt. 4 ss. c.p.p.

[8] La stessa legge, all'art. 12-bis, ha dettato una specifica disciplina transitoria, aggiungendo, all'art. 11 della l. n. 48 del 2008, un nuovo comma 1-bis, a norma del quale "*le disposizioni di cui al comma 3-quinquies dell'art. 51 del c.p.p., introdotto dal comma 1 del presente articolo, si applicano solo ai procedimenti iscritti nel registro di cui all'art. 335 del c.p.p. successivamente alla data di entrata in vigore della presente legge*".

riguardo alla competenza territoriale.

Tuttavia molti erano i profili di criticità dal punto di vista costituzionale, i quali probabilmente avrebbero potuto fondare un solido ricorso alla Consulta.

La ripartizione delle competenze territoriali realizzata dalla l. 48/2008 contrastava manifestamente con il canone di ragionevolezza per come elaborato nel corso degli anni dalla giurisprudenza costituzionale, non sussistendo alcuna giustificazione logico-razionale che potesse motivare un simile impianto. La situazione di incertezza che veniva a crearsi appariva in contrasto con la garanzia costituzionale del giudice naturale precostituito per legge (art. 25, c. 1 Cost.), e conseguentemente con i valori fondamentali della difesa (art. 24, c. 2 Cost.), pure lesi da un'eventuale declaratoria di incompetenza in negativo, dal momento che da una siffatta pronuncia sarebbe derivata l'assoluta impossibilità per l'indagato di difendersi attivamente. Sussisteva anche il rischio di rendere meno efficiente l'amministrazione della giustizia, così ledendo il principio generale del buon andamento degli uffici della pubblica amministrazione *ex* art. 97 e rendendo più difficoltoso l'esercizio dell'azione penale, obbligatorio a norma dell'art. 112 Cost.; venivano infine compromessi anche i tempi del processo, del quale va assicurata la ragionevole durata *ex* art. 111, c. 2. L'originario riparto della competenza territoriale in tema di reati informatici avrebbe costituito un irragionevole sacrificio di valori costituzionali, non bilanciato da esigenze di tutela di beni di rango superiore o almeno equivalente a quelli citati[9]. La Corte di Cassazione non avrebbe potuto porre rimedio al difetto di coordinamento neanche con un'interpretazione adeguatrice costituzionalmente conforme: sarebbe stato un tentativo quanto mai forzato, poiché la Costituzione pone chiaramente un'altra norma, l'art. 25 c. 1 Cost., che vieta tassativamente deroghe alla competenza del giudice naturale se non per mezzo di legge anteriore al fatto commesso.

L'unica vera alternativa all'applicazione della disciplina della competenza territoriale "asimmetrica" sarebbe stata quindi sollevare questione di legittimità costituzionale innanzi alla Consulta.

[9] M. Giuseppe, "*La competenza territoriale in materia di reati informatici, fra giurisdizione di legittimità e profili di incostituzionalità: brevi note a margine della sent. Cass. Pen. n. 45078/2008*" in www.diritto.it (2009).

Se questo *impasse* è stato positivamente risolto dall'intervento correttivo del legislatore, permangono difficoltà di coordinamento fra la competenza distrettuale prevista per la frode informatica e la competenza ordinaria prevista per la fattispecie limitrofa di "indebito utilizzo di carte di credito o pagamento" di cui alla normativa antiriciclaggio (D.lgs. n. 231/2007). In questo secondo caso, la competenza territoriale deve essere determinata sulla base delle ordinarie regole, non sussistendo alcuna disciplina derogatoria: perciò competente sarà il giudice del luogo in cui è avvenuta una delle condotte fraudolente previste dalla disposizione, ex art. 8 c.p.p. ovvero il giudice determinato sulla base degli ulteriori criteri previsti agli artt. 9 e segg. c.p.p..

Il problema nasce dalla difficoltà di individuare la *ratio* della scelta del legislatore di differenziare sia l'attribuzione del trattamento delle indagini relativamente alle due fattispecie sia la procedibilità: perché il legislatore ha deciso di devolvere sì al G.I.P. – G.U.P. distrettuale ma solo su querela dell'offeso la competenza relativamente al delitto di frode informatica e mantenere per la fattispecie di indebito utilizzo la competenza a livello locale con però procedibilità d'ufficio?

Si tratta di due fattispecie non così diverse dal punto di vista dell'offensività della condotta o delle competenze specialistiche richieste per l'accertamento, stante la natura *latu sensu* informatica anche dell'indebito utilizzo di strumenti di pagamento.

Non è difficile immaginare le frizioni a livello applicativo derivanti dalle indagini relative alle due fattispecie: potrà ben accadere che due Procure, l'una competente ad indagare sul delitto di indebito utilizzo in base alle regole ordinarie, l'altra sulla frode informatica in base alla disciplina derogatoria di cui all'art. 51 comma 3-*quinquies* c.p.p., si ritrovino a procedere in maniera del tutto indipendente ed autonoma nell'attività di ricerca della prova sullo stesso fatto materiale. I problemi non diminuiscono nel caso in cui le indagini riguardino casi di concorso fra i due delitti in commento: Procura Locale e Procura Distrettuale potrebbero ritrovarsi ad indagare ognuna singolarmente su fatti che, dal punto di vista della fenomenologia dell'offesa, richiederebbero un *iter* investigativo congiunto. Conseguentemente si creerebbe la probabilità di duplicare inutilmente i costi e i tempi delle indagini, finendo a causare nocumento altresì

ai diritti della difesa nonché dei soggetti coinvolti.

La duplicazione della fase investigativa dovrebbe essere risolta dal successivo intervento del giudice competente per il reato "più grave", essendo di fronte ad un caso di connessione di procedimenti ex art. 12 c.p.p.. A questo punto tuttavia sarebbe necessario aprire il dibattito su quale risulti il delitto più grave fra i due: dal punto di vista delle ipotesi-base, risulta più grave la fattispecie prevista dalla legislazione speciale, stante la cornice edittale più elevata e la perseguibilità d'ufficio. Tuttavia se venisse contestata una forma aggravata di frode informatica ex comma 2 art. 640-ter c.p. il problema sarebbe più complesso, poiché la cornice edittale prevista sarebbe pressoché la medesima: l'unica differenza nella sanzione si rinviene in pochi centesimi di scarto nella multa, che potrebbero però essere interpretati come un mancato arrotondamento per difetto nella fattispecie codicistica[10]. La prevalenza sarebbe comunque sempre da accordare alla fattispecie speciale, pur essendo di competenza locale.

Ne risulterebbe ancor meno giustificata la competenza distrettuale della frode informatica, dato che una fattispecie limitrofa che richiede altrettante competenze tecniche specialistiche soggiace alle regole ordinarie di determinazione della competenza territoriale. A seconda della contestazione mossa dall'organo dell'accusa la competenza risulterebbe radicata a livello distrettuale ovvero a livello territoriale ordinario, con necessità di trasferire materialmente tutta la documentazione raccolta se il giudice dovesse riqualificare il fatto nell'uno o nell'altro senso.

Dal canto suo la giurisprudenza sembra aver voluto dare una risposta in proposito, sulla base di una supposta *vis attractiva* della competenza distrettuale individuata relativamente all'art. 51 c. 3-*bis* c.p.p.: la competenza funzionale ha valore prioritario, determinandosi come deroga "*assoluta ed esclusiva*" agli ordinari canoni di determinazione della competenza per territorio con prevalenza dell'attribuzione al magistrato del capoluogo su qualunque altra regola di individuazione della stessa, purché sia accertato il luogo di

[10] Nel caso di frode informatica commessa con furto o indebito utilizzo di identità digitale (comma 3 art. 640-ter c.p.) la risoluzione della questione relativa alla fattispecie più grave sarebbe più agevole, dato che la cornice edittale prevista nella nuova aggravante del 2013 è sensibilmente più elevata anche rispetto alla fattispecie extracodicistica. In questo specifico caso perciò la competenza sarebbe determinata con prevalenza dell'aggravante codicistica.

consumazione degli altri reati. Conseguentemente, la competenza "generale" va individuata sulla base dei reati inclusi nel catalogo di cui all'art. 51 c. 3-*bis* c.p.p: eventuali ulteriori reati connessi, quand'anche più gravi e commessi fuori distretto, risentirebbero di questa particolare deroga individuata dall'art. 51 c.p.p. e confluirebbero in via derivata nell'ambito operativo distrettuale[11].

Tale orientamento dei giudici, che ha il merito di cercare una soluzione argomentata ad un problema di diritto vivente che non attira l'attenzione del legislatore, conduce tuttavia a risultati diametralmente opposti rispetto a quelli risultanti dal meccanismo della competenza per connessione ex art. 12 c.p.p.. Le perplessità suscitate sono varie e di rilievo: in primis non si comprende come la competenza funzionale possa incidere sulla competenza territoriale, non essendoci nessuna deroga espressamente prevista nell'ordinamento, né un principio per il quale la competenza funzionale sia "più importante" e prevalente rispetto a quella territoriale[12]. Dall'altra però sembra come minimo poco razionale che l'applicazione della regola ordinaria finisca per dare rilievo ad un reato diverso da quelli inclusi nel catalogo di cui all'art. 51 c.p.p.: viene sconfessato l'impianto fondamentale che considera la competenza funzionale come originaria. Infine, non si può non notare come l'orientamento giurisprudenziale in commento sia nato e sia poi stato condiviso limitatamente alle fattispecie previste al comma 3-*bis* dell'art. 51 c.p.p.: si tratta di fenomeni logicamente differenti dai reati informatici, attribuiti alla Procura Distrettuale per ragioni tutt'affatto diverse da quelle che hanno motivato l'introduzione nello stesso articolo del comma 3-*quinquies* nel 2008.

La stessa Suprema Corte è recentemente intervenuta a ridimensionare il proprio orientamento interpretativo relativamente all'art. 51 c.p.p., sottolineando proprio come le sue passate pronunce abbiano sempre riguardato reati di cui all'elenco previsto al comma 3-*bis* dell'articolo sopracitato, caratterizzati dal vincolo associativo: perciò sarebbe la natura stessa del reato e non la sua mera inclusione nell'art. 51 c.p.p. a determinare la *vis attractiva* derogatoria di

[11] Cass. Pen., sez. II, sent. n. 6783 del 17/02/2009; Cass. Pen., sez. II, sent. n. 19831 del 9/06/2006, *Mohammad*; Cass. Pen., sez. IV, sent. n. 17386 del 19/05/2006; Cass. Pen., 18/05/2005, *Daiu*, in Cass. Pen. 2006. Si tratta dell'orientamento prevalente in giurisprudenza, seguito dalla maggior parte delle Procure, inclusa quella di Trento.

[12] G. Spangher, "*Trattato di procedura penale – 1. soggetti e atti*", UTET, 2009, p. 100.

competenza, costituendo il reato associativo "*in qualche modo il collante ed il collettore di tutti i diversi reati-fine ad esso connessi, (non a caso, nella pratica, in queste ipotesi si parla di reati satellite) sì da costituire il momento logicamente unificante di essi, quand'anche si tratti di reati che unitariamente intesi potrebbero essere più gravi di quello associativo*"[13].

È la stessa Corte quindi che limita la supposta forza attrattiva della deroga di cui all'art. 51 c.p.p., sostenendo che sia legittimata dalla fenomenologia dei reati associativi previsti al comma 3-*bis*.

Peraltro, la Corte non sconfessa completamente il proprio passato orientamento: nel caso di fattispecie non caratterizzate dalla struttura associativa, il trasferimento della funzione inquirente in sede distrettuale opera sì ma solo entro i limiti del distretto. La competenza dovrà in primis essere individuata sulla base degli ordinari criteri, poiché altrimenti il rischio è quello di distogliere dal "*giudice naturale precostituito per legge*", con violazione degli art. 24 e 25 Cost. In tal modo però si crea una disparità di trattamento fra delitti connessi che si verificano all'interno del medesimo distretto e delitti altrettanto connessi che si verificano però *extra-districtum*.

In conclusione, la scelta di attribuire la fase investigativa relativamente ai reati informatici alla Procura Distrettuale ha destato varie fondate perplessità e causato problemi di coordinamento con le indagini relative ad altri delitti, che spesso si verificano in concorso o risultano a vario titolo connessi. La Suprema Corte ha tentato di dare una sistemazione organica all'impianto, ma le argomentazioni proposte sono spesso contestabili poiché si scontrano con dati normativi che poggiano su basi poco solide. È quindi auspicabile un intervento del legislatore, che dia una nuova disciplina organica per i casi in cui sia coinvolta l'azione della Procura Distrettuale o per lo meno avvalli il percorso argomentativo dei giudici di legittimità, stabilendo *ex lege* la prevalenza della competenza distrettuale rispetto a quelle dei reati connessi.

[13] Cass. Pen., sez. III, sent. n. 52512 del 22/05/2014: "*La deroga apparirebbe del tutto ingiustificata laddove il reato di competenza distrettuale non abbia una siffatta peculiare valenza, ma si presenti semplicemente come uno dei diversi reati connessi*".

5.2. Le nuove frontiere della concezione di sistema informatico

Punto di particolare interesse nello sviluppo delle applicazioni della fattispecie di frode informatica sono gli innovativi ampliamenti del concetto di "*sistema informatico o telematico*". Fin dalle prime applicazioni, la giurisprudenza è stata consapevole del fatto che si trattava dell'elemento più di tutti caratterizzante la fattispecie; ha così dimostrato di interpretare tale nozione in un'accezione molto ampia, di modo tale da far vivere la fattispecie in commento in contesti molto variegati fra loro, adattandola allo sviluppo tecnologico-sociale. Sono venuti prima in considerazione gli elaboratori elettronici di dati sia degli apparati governativi, sia considerati come *Personal Computer* in senso stretto, passando poi ad ampliare il raggio d'azione includendo le "centraline telefoniche" e la rete telefonica: queste sono state ritenute sistema informatico-telematico poiché, tecnicamente, il trasporto delle informazioni in rete avviene in forma numerica (avendosi quindi attività di codificazione e decodificazione) attraverso impulsi elettronici, i c.d. *bit*, con un procedimento automatizzato che abilita l'utilizzo delle linee per la chiamata solo di determinate utenze[14].

Partendo da questa interpretazione della nozione in commento, la giurisprudenza prima di merito e poi anche di legittimità ha ravvisato un sistema telematico nella rete di telefonia mobile, sanzionando ex art. 615-quater c.p. l'uso di un apparecchio telefonico clonato per realizzare un'illecita connessione alla stessa in danno di ignari utenti: i numeri telefonici ed i numeri seriali dei cellulari sono stati considerati quindi codici di accesso ad un vero e proprio sistema telematico[15].

Già alcune pronunce della fine degli anni novanta hanno fornito un'analisi del rapporto tra sistema informatico-telematico e gli strumenti di telefonia. Infatti, nella sentenza di Cassazione "*De Vecchis*" si sottolineava come, poiché l'espressione "*sistema informatico*" di cui all'art. 640-ter c.p. si riferisce ad una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile

[14] Cass. Pen., sez. VI, sent. n. 3065 del 14/12/1999, ud. 4/10/1999, "*De Vecchis*".
[15] F. Vitale, "*Brevi riflessioni sul reato di "frode informatica: i servizi a contenuto applicati dalle compagnie telefoniche nell'alveo dei cyber crime*", in Archivio penale, n. 1, www.archiviopenale.it.

all'uomo attraverso l'utilizzazione (anche in parte) di tecnologie informatiche, deve ritenersi che sia la rete telefonica di cui si serve Telecom, sia il centralino di una singola filiale costituiscono un sistema che si avvale di tecnologie informatiche, perciò oggetto immediato della condotta fraudolenta.

Come già accennato nei paragrafi precedenti[16], la definizione di "computer" va aggiornata ed attualizzata; e in questa direzione ha cercato negli anni di muoversi la giurisprudenza, la quale ha avvertito da un lato le grandi potenzialità dell'art. 640-ter c.p., costruito in termini così ampi, dall'altro le diverse istanze di tutela emergenti nelle aule di giustizia rispetto all'uso fraudolento delle nuove tecnologie. Il percorso intrapreso con la sentenza "*De Vecchis*" del 1999 ha sancito la non necessaria presenza di una totale utilizzazione di tecnologie informatiche da parte del c.d. sistema informatico o telematico, prendendo atto dello sviluppo tecnologico grazie al quale oggi, servendosi delle sofisticate nanotecnologie, sono proprio gli strumenti ed oggetti più comuni ad avere in sé una componente informatica: praticamente ogni bene può essere automatizzato, debitamente programmandolo ad una funzione attraverso l'inserimento di un *micro-chip*, che è a tutti gli effetti un micro sistema informatico. Qualsiasi *smartphone*, qualsiasi distributore automatico di beni o servizi deve essere considerato un sistema automatico, nella misura in cui risulti funzionante attraverso un elaboratore elettronico di dati: ciò che risulta necessario e sufficiente a tal fine è che sia stato inserito nell'oggetto in questione un *chip* programmato per elaborare in maniera automatizzata dei dati cui segue lo svolgimento della specifica funzione utile all'uomo.

L'alterazione di un sistema informatico o telematico si configurerà tutte le volte in cui sia verificata una manipolazione, che abbia modificato, fraudolentemente, il regolare modo di operare del (micro)sistema, facendo così svolgere alla macchina funzioni non legittimamente programmate.

Viene in evidenza oggi il caso avente ad oggetto il fraudolento "attacco" al credito delle utenze telefoniche mobili attraverso servizi non richiesti: si tratta della problematica relativa ai cc.dd. "servizi premium" che migliaia di utenti,

[16] Cap. II par. 5

navigando su internet con i propri dispositivi, o semplicemente utilizzando applicazioni del proprio *smartphone* o *tablet* si ritrovano improvvisamente e senza saperlo ad aver attivato senza mai aver richiesto; ricevono così contenuti vari in abbonamento, vedendosi applicati dalle compagnie telefoniche costi piuttosto elevati. Oltre alla tutela garantita dal diritto dell'Antitrust di fronte a pratiche commerciali scorrette e comportamenti commerciali aggressivi, può essere rinvenuta la condotta di cui all'art. 640-ter c.p. sotto il profilo della tutela penale del patrimonio del privato nei rapporti contrattuali: le alterazioni dei sistemi informatici o telematici consistono, per lo più, in vere e proprie manipolazioni dei programmi, ovverosia dei *software*, che i computer (e altresì gli strumenti moderni di telefonia mobile, a tutti gli effetti considerabili dei piccoli ed autonomi sistemi informatici) utilizzano per elaborare dati ed informazioni e possono essere commesse sia attraverso la parziale o totale modificazione del programma, normalmente e regolarmente utilizzato, sia attraverso la giustapposizione, sovrapposizione o contrapposizione a quest'ultimo di altri programmi autoinstallanti attraverso la Rete.

Sempre per tutelare il consumatore spesso poco attento rispetto ai molti stratagemmi di guadagno posti in essere dai *cyber criminal*, nel 2011 e poi anche nel 2012[17], la Corte di Cassazione ha utilizzato la fattispecie di frode informatica per colpire le operazioni di clonazione di carta di credito effettuate attraverso l'utilizzo di "*skimmer*": con tale apparecchio per la lettura e la memorizzazione dei contenuti presenti sulle bande magnetiche delle carte elettroniche, il frodatore entra in possesso dei dati delle carte di pagamento, codice PIN incluso (in caso di bancomat o carta di credito), per poi penetrare abusivamente nel sistema bancario, considerato a tutti gli effetti un sistema telematico, ed effettuare operazioni illecite di trasferimento di denaro.

Nell'iter applicativo dell'art. 640-ter c.p. sono così state affrontate problematiche molto diverse fra loro, proprio grazie all'estrema ampiezza e duttilità delle formule utilizzate nella composizione della fattispecie e al suo collocarsi in maniera non proprio netta dal punto di vista dell'oggetto giuridico tutelato, per

[17] Cass. Pen., sez. II, sent. n. 17748 del 6/05/2011; Cass. Pen., sez. II, sent. 11699 del 10/01-28/03/2012.

alcuni esclusivamente di tipo privatistico, per altri con una connotazione pubblicistica. Considerando anche solo l'ambito più strettamente privatistico di applicazione della fattispecie in commento, risulta evidente la poliedricità dell'art. 640-ter c.p., in quanto da un lato si pone come presidio penale rispetto ad abusi propriamente patrimoniali posti in essere mediante lo strumento informatico, tutelando in maniera derivata anche la trasparenza e l'affidabilità degli scambi, dall'altra – attraverso la nuova aggravante del 2013 – la norma assume una connotazione personalistica, risultando un utile garanzia per le molteplici proiezioni personali nella realtà informatica consistenti nella c.d. identità digitale. L'autorità giudiziaria è chiamata a dare una risposta sanzionatoria effettiva sia alle istanze del consumatore-utente, soggetto privato spesso poco esperto ed inerme di fronte alla fervida fantasia del criminale informatico, sia alle istanze dello Stato o di un altro ente pubblico spesso presi di mira da frodi e attacchi informatici sofisticati.

In particolare, la giurisprudenza della Suprema Corte è giunta recentemente a ravvisare un'ipotesi di frode informatica nella manomissione delle cc.dd. *slot machine*, al fine di maggior guadagno, attraverso l'elusione dell'imposta dovuta al fisco[18].

Si è così ritenuta sussistente la violazione dell'art. 640-ter c.p. nella condotta di inserimento nelle cc.dd. *slot machine* di una seconda scheda che andasse a modificarne fisicamente la modalità di funzionamento. All'interno della macchina da gioco è regolarmente montata una scheda su cui è installato un *micro-chip*, processore su cui sono registrate le istruzioni che le permettono di svolgere la funzione di intrattenimento per cui è programmata: di conseguenza, una condotta fraudolenta alterativa dello stesso costituisce un'alterazione del funzionamento del sistema informatico rilevante ai sensi dell'art. 640-ter c.p.

Nella sentenza n. 27135 del 2010, i giudici di Cassazione hanno sottolineato come "*Non rileva il fatto che il software contenuto nella scheda originaria sia rimasto inalterato e possa operare regolarmente una volta riattivato: ciò che risulta alterato, nel caso in esame, è il funzionamento del sistema informatico*

[18] Cass. Pen., sez. V, sent. n. 27135 del 19/03/2010 (dep. 13/07/2010); Cass. Pen., sez. II, sent. n. 18909 del 30/04/2013.

nel suo complesso, in dipendenza della sostituzione del software con altro diversamente operante: a ciò non essendo di ostacolo la reversibilità della modifica". Perciò, nel caso in cui venga introdotta in un qualsiasi tipo di apparecchio elettronico automatizzato una seconda scheda attivabile a distanza che lo abiliti all'esercizio di una funzione diversa da quella prevista dal programmatore o utilizzatore dello stesso, si verifica una condotta rilevante ai sensi dell'art. 640-ter c.p., che si sostanzia nell'attivazione di un diverso programma con conseguente alterazione del funzionamento del sistema informatico nel suo complesso. E non rileva verificare la reversibilità della situazione illegittimamente modificata o la non continuità dell'alterazione.

L'elemento tipico dell'ingiusto profitto con altrui danno, nel caso di cui ci si occupa, è ravvisato nell'esercizio del gioco d'azzardo senza che venga assoggettato al controllo telematico e alla conseguente tassazione proporzionale: la tutela del patrimonio apprestata dall'art. 640-ter c.p. diventa efficace presidio anche per le entrate fiscali, nella forma di frode informatica aggravata ai danni dello Stato, poiché l'alterazione degli apparecchi elettronici destinati a "giochi di abilità" e trasformati in slot machine comporta la fraudolenta elusione della maggiore imposta proporzionale quantificata nel 13,5% dei proventi[19].

Nella sentenza n. 18909 del 2013, i giudici di Cassazione affrontano anche il conseguente problema del rapporto con il delitto di peculato, prima fattispecie posta a presidio del patrimonio dell'ente pubblico dai potenziali abusi dei pubblici ufficiali ed incaricati di pubblico servizio. Nel caso in esame viene esclusa la sussistenza del delitto di cui all'art. 314 c.p., poiché l'alterazione del sistema informatico è l'elemento caratterizzante, necessario e sufficiente ai fini della consumazione del reato: è il possesso stesso del profitto ad essere indebito, essendo proprio grazie all'alterazione del *software* che il gestore, in concorso con i concessionari del servizio nasconde al fisco le maggiori entrate determinate dal gioco d'azzardo. A seguito della suddetta condotta fraudolenta, il Monopolio di Stato, al quale avrebbe dovuto essere versata la percentuale del

[19] Nel caso trattato dai giudici di legittimità nel 2013 il denaro risultava trattenuto illecitamente dal gestore e dagli stessi concessionari che lo avevano aiutato a nascondere gli apparecchi all'Erario.

13,5% delle somme giocate, non poteva essere a conoscenza dei maggiori guadagni dell'agente, quindi non era nelle condizioni di riscuotere l'imposta dovuta; la percentuale del 13,5% è stata incassata e trattenuta illecitamente da coloro che avevano alterato il sistema informatico. La fattispecie di peculato invece si sarebbe potuta ravvisare se l'ufficiale o incaricato di pubblico servizio avesse avuto legittimamente la disponibilità della *res* e se ne fosse quindi impossessato, ponendo successivamente in essere una condotta manipolativa per occultare la appropriazione. Lo Stato in tal caso sarebbe messo nelle condizioni di controllare le giocate e di quantificare il tributo dovuto, e sarebbe necessaria una successiva condotta fraudolenta dell'agente per nascondere il mancato versamento fiscale[20].

Ecco che in tal caso la frode informatica supplisce al vuoto di tutela che sarebbe lasciato dalla impossibilità di applicare la fattispecie prevista specificamente per gli abusi da parte del funzionario pubblico: l'art. 640-ter c.p. e l'art. 314 c.p. risultano quindi caratterizzati ognuno da un autonomo ambito di operatività.

5.3. Il *Phishing*

Uno dei più pericolosi fenomeni illeciti degli ultimi anni è il "*phishing*", che ha assunto velocemente una portata internazionale proprio nella sua connotazione informatica: si tratta della "tecnica perfetta" per sfruttare, da un lato, le debolezze investigative e repressive determinate dai confini delle giurisdizioni statali e, dall'altro, l'ignoranza o la semplice ingenuità degli utenti della rete[21].

---

[20] "*L'elemento distintivo va individuato con riferimento alle modalità del possesso del denaro o d'altra cosa mobile altrui oggetto di appropriazione, ricorrendo il reato di peculato quando il pubblico ufficiale o l'incaricato di pubblico servizio se ne appropri avendone già il possesso o comunque la disponibilità per ragione del suo ufficio o servizio, e ravvisandosi invece il reato di frode informatica quando il soggetto attivo, non avendo tale possesso, se lo procuri fraudolentemente, facendo ricorso ad artifici o raggiri per procurarsi un ingiusto profitto con altrui danno*"; così in Cass. Pen., sez. II, sent. 18909 del 30/04/2013.

[21] Esistono varie tecniche di phishing, tutte accomunate dall'effetto finale, che consiste nel farsi consegnare o sottrarre con l'inganno dati o informazioni personali sensibili, al fine di trarne profitto. La maggior parte sfrutta la rete di contatti e l'anonimato garantiti da Internet oppure le debolezze dei singoli elaboratori ovvero dei sistemi aziendali (attraverso l'invio di e-mail, il

Il “phishing” non ha una conformazione fattuale precisa e stabilita una volta per tutte, né un target determinato: si tratta di un fenomeno in continua evoluzione che subisce metamorfosi continue non solo per la necessità di individuare tecniche d’inganno sempre nuove e credibili ma altresì grazie allo sviluppo delle tecnologie, che rende in breve tempo obsoleti gli strumenti in uso e permette anche ai criminali di avvalersi di risorse sempre più sofisticate (e pericolose). Può colpire qualsiasi tipo di utente finale, dal soggetto privato inesperto nella sua postazione domestica, alla piccola, media o grande impresa, all’istituto di credito o assicurativo, all’agenzia di money transfer, all’ente pubblico: tutti senza distinzione possono rimanere vittima di questa condotta fraudolenta, il cui unico fine è generare indebiti profitti attraverso l’utilizzo fraudolento di informazioni altrui. Ciò posto, trattandosi di un fenomeno socio-criminologico di derivazione empirica, non è possibile inquadrare il “phishing” in una determinata fattispecie astratta: e ciò sia poiché non è possibile individuare a priori delle condotte tipiche che, sole, conducano al risultato che il *phishers* si prefigge, ma anche per il fatto che spesso nei fatti si manifesta come condotta composita, la quale assume rilevanza penale nella forma del reato associativo, necessariamente continuato, sussistendo più condotte illecite, astrattamente distinguibili a seconda della fase dell’attacco, teleologicamente orientate alla realizzazione del “medesimo disegno criminoso” ex art. 81 c.p..

Gli attacchi di “phishing” e similari ormai da alcuni anni (almeno dal 2007-2008) sono in costante aumento su scala internazionale[22], merito probabilmente delle

---

download surrettizio di programmi malevoli o il dirottamento di comunicazioni riservate); tuttavia si registrano casi nei quali la “pesca di dati” è avvenuta a voce (c.d. “*vishing*”, contrazione di “voice-phishing”) attraverso telefonate di fantomatici operatori, cui l’utente è indotto con l’inganno a comunicare dati sensibili.

tute accomunate dall’effetto finale, che consiste nel farsi consegnare o sottrarre con l’inganno dati o informazioni personali sensibili, al fine di trarne profitto.

[22] Non vi sono dati ufficiali sui casi di phishing in Italia: vi sono tuttavia numerosi gruppi di lavoro, organizzazioni e aziende private che si occupano di stilare statistiche e condurre sondaggi, mostrando un trend di assoluta ascesa e pericolosità del fenomeno.

Dai primi report disponibili al sito http://www.anti-phishing.it/ sono emersi dati allarmanti con riguardo alla rapidissima crescita degli attacchi di phishing contro obiettivi italiani: le prime rilevazioni hanno registrato una crescita dal primo trimestre del 2006 rispetto al primo trimestre del 2007 del +1.775%, registrando 225 attacchi totali. Nella seconda rilevazione (aprile-giugno 2007) il numero totale dei casi è passato a 2115, con una crescita rispetto al primo trimestre del 2007 del +940% e una media di 23,24 tentativi giornalieri.

Nei primi sei mesi dell'anno 2013 l’azienda di cyber security e formazione D3Lab (https://www.d3lab.net/index.php/blog/126-stat-1-sem-2013) ha rilevato 1247 differenti URL

potenzialità di profitto a fronte di costi e rischi pacificamente sostenibili, uniti alla possibilità di spersonalizzare l'attacco, godendo del pieno anonimato nei confronti del reo-vittima. Anche il mondo della criminalità organizzata transnazionale, resosi conto delle potenzialità di guadagno insite nel "phishing", ha incominciato a sfruttarlo, come fonte di impulso e mezzo di finanziamento[23].

In linea generale si può affermare che il phishing assume la caratterizzazione di un vero e proprio attacco informatico, rivolto agli utenti della rete e ai sistemi informatici e telematici, i cui elementi essenziali sono il furto di dati sensibili e il loro utilizzo del tutto indebito, per lo più al fine di operare trasferimenti illeciti di denaro o riciclare denaro proveniente da attività illecite.

Lo stesso termine *phishing* secondo alcuni evoca l'immagine della "pesca", poiché deriverebbe dalla storpiatura del verbo inglese *to fish*, nella accezione di "pescare utenti nella rete Internet", pronti ad abboccare agli stratagemmi sviluppati dagli hackers[24]. Per altri il termine sarebbe una crasi, un collage di tre parole inglesi, "*password*", "*harvesting*" e "*fishing*", ed indicherebbe la raccolta, effettuata pescando, di parole chiave e codici d'accesso a servizi economico-finanziari[25].

---

fraudolente di attacco. In più di un caso tali URL sono state riutilizzate più volte consecutivamente, anche a distanza di diversi mesi. Il confronto degli attacchi portati ai vari enti conferma Poste Italiane quale ente maggiormente colpito dai criminali (578 attacchi su 1247), sempre interessati alla conquista dei dati degli account Poste Pay, mentre Carta Sì, altra impresa particolarmente colpita negli anni, può vantare una forte contrazione di attacchi in questi primi sei mesi, rimanendo comunque fortemente colpita (da 151 attacchi trimestrali nel 2012 a 97 nel primo trim. 2007). Da un sondaggio web condotto da Sophos (https://www.sophos.com/it-it/press-office/press-releases/2006/04/pr_it_phishstats.aspx), che ha coinvolto oltre 600 utenti business, è emerso che il 58% riceve almeno una mail di phishing al giorno, mentre un allarmante 22% ne riceve più di cinque al giorno, a conferma della rilevante crescita del fenomeno. Recenti statistiche del Gruppo di Lavoro internazionale Anti-Phishing (APWG) del quale fa parte anche Sophos, rivela che sono stati individuati 13.562 tentativi di phishing nel settembre 2005 e 15.244 nel mese di dicembre 2005, mentre nel dicembre 2004 ne erano stati riscontrati 8.819. Gli Stati Uniti si confermano il Paese più colpito, seguiti da Cina e Corea.

[23] Nel 2007 le indagini della Procura di Milano hanno consentito di identificare due diverse associazioni a delinquere che "riferivano" a soggetti in Romania, dedite sistematicamente all'attività di phishing. F. Cajani, G. Costabile, G. Mazzaraco, "*Phishing e furto di identità digitale – indagini informatiche e sicurezza bancaria*", 2008, Giuffré, pag. 188.

[24] "*The term 'phishing' comes from the analogy that Internet scammers are using e-mail lures to 'fish' for passwords and financial data from the sea of Internet users. The term was used by the mid 1990's to describe tricking Internet users to reveal their passwords for dial-up service*", in "*A Call for action, Report from the national consumers league, Anti-phishing Retreat*", marzo 2006.

[25] S. Frattallone, "*Phishing, fenomenologia e profili penali: dalla nuova frode telematica al cyber riciclaggio*", in Global Trust, www.globaltrust.it/documents/press/phishing/;

Si tratta di un fenomeno che sfrutta tecniche di *social engineering*[26], sostanziandosi – nella sua forma più diffusa – nell'invio da parte di ignoti truffatori di messaggi di posta elettronica ingannevoli, attraverso i quali le vittime designate sono indotte a fornire volontariamente all'estraneo proprie informazioni confidenziali. In tal modo, i frodatori non corrono il rischio – tendenzialmente molto elevato – insito nel tentativo di forzare il sistema informatico centrale di un istituto di credito, una grande impresa ovvero di un ente pubblico economico, affrontandone le misure di sicurezza e i sistemi di rilevazione di effrazione digitale: semplicemente spostando il bersaglio d'attacco, si hanno maggiori possibilità di raggiungere comunque l'obiettivo (il profitto economico)[27], ma il pericolo di fallimento e/o di sanzione è drasticamente ridotto. La tecnica del "phishing" permette perciò di colpire il vero anello debole delle transazioni telematiche, vale a dire il consumatore-utente telematico, e guadagnare in maniera più semplice e immediata: da un lato infatti, il grado di tecnologia necessario per nascondere le proprie tracce ad un utente medio ed evitare così di essere rintracciati non è così elevato come può essere quello richiesto nel contesto di un attacco ad un infrastruttura informatica aziendale altamente sofisticata; dall'altro, attaccando il singolo utente, l'hacker può avvantaggiarsi anche della sua mancanza di conoscenze e capacità tecniche specifiche, consentendogli di non essere riconosciuto e agire indisturbato. Cionondimeno, è bene sottolineare come l'arma fondamentale del phisher non si sostanzi in una specifica risorsa tecnologica, bensì risulti la sua

[26] Per ingegneria sociale si intende lo studio del comportamento individuale di una persona al fine di carpire informazioni. Può essere un modo sorprendentemente efficace per ottenere la chiave crittografica di un sistema, soprattutto se comparato con altri. Con l'evoluzione dei software, l'uomo ha migliorato i programmi a tal punto che essi presentano pochissimi *bug* (errori di programmazione): perciò spesso per un *hacker* è pressoché impossibile attaccare un sistema informatico, non riuscendo a scoprirne le debolezze. L'unico sistema davvero proficuo per procurarsi le informazioni necessarie è attuare un attacco di ingegneria sociale, vale a dire saper mentire per carpire fraudolentemente informazioni chiave. Un ingegnere sociale per definirsi tale deve saper fingere, saper ingannare gli altri: deve essere abile a nascondere la propria identità, poiché solo in tal modo riesce a ricavare le informazioni più private. Nel caso sia un hacker, può assumere informazioni inerenti ad un sistema informatico o telematico: infatti, nella maggior parte dei casi, il cosiddetto ingegnere riesce a ricavare tutto ciò che gli serve dalla vittima ignara. Da *Wikipedia*, l'enciclopedia libera: http://it.wikipedia.org/wiki/

[27] Le maggiori possibilità di guadagno derivano dal fatto che il *phisher*, una volta ottenute le informazioni personali delle vittime, non dovrà compiere un accesso intrinsecamente fraudolento o trovare il modo per aggirare le misure di sicurezza del sistema: dispondendo della "chiave", i movimenti patrimoniali posti in essere in apparenza saranno del tutto legittimi, proprio grazie all'utilizzo delle credenziali fornite dalla stessa vittima.

vis persuasiva, la sua capacità di confezionare un messaggio (per e-mail o attraverso qualsiasi altro strumento) in grado di carpire la fiducia dell'utente, che in tal modo conferirà volontariamente i propri dati.

Come già accennato, nella forma più diffusa il "phishing" trae origine dall'invio randomico a migliaia di destinatari di e-mail, in apparenza provenienti da un mittente legittimo e conosciuto all'utente per lo meno per fama (*spamming*)[28]. I messaggi solitamente segnalano presunti problemi tecnici del sistema informatico del mittente, procedure di aggiornamento software, tentativi di accesso fraudolento o addirittura vengono motivati con la necessità di prevenire il rischio di eventuali future frodi ai danni dei propri clienti: in tutti i casi comunque il messaggio contiene un "invito all'azione" e il cliente è indotto, attraverso i toni allarmanti delle segnalazioni inviate, a dare proprie informazioni sensibili, come dati anagrafici, residenza, coordinate bancarie ovvero i propri codici identificativi ed operativi. La procedura "guidata" viene azionata accedendo alla pagina web puntata da un link di regola contenuto nella stessa e-mail: lo stato di costrizione psicologica nel quale il destinatario si trova nasce dalla formalità del messaggio inviato, che in tutto e per tutto appare uguale a quelli inviati dall'ente o Istituto legittimo, mescolata ai toni allarmanti che causano ansia nel cliente rispetto alle ipotetiche conseguenze in cui rischia di incorrere[29].

Si parla generalmente di "*deceptive phishing*": l'utente un poco ingenuo si affretta a visualizzare la pagina web cui invia il link contenuto nel messaggio, che appare perfettamente (o quasi, ma spesso si tratta di differenze di dettaglio o relative ad aspetti particolarmente tecnici, che non sono il pane quotidiano dell'utente medio) identica a quella originale dell'istituto di credito o altro mittente, replicando l'originale impostazione grafica, l'eventuale marchio e il tenore linguistico e lessicale di una comunicazione standard cui l'utente è

[28] Si tratta di enti, istituti ed organizzazioni cui il consumatore medio è avvezzo e che, avendo essi centinaia di migliaia di clienti, con molta probabilità intrattengono un qualche tipo di relazione contrattuale con la vittima designata: fra gli istituti di credito spiccano Unicredit, Intesa SanPaolo, Banca Intesa, Banca Fideuram, Credem, Banca Mediolanum e IwBank; Fineco fra le imprese di concessione prestiti; particolarmente colpite sono l'impresa a partecipazione pubblica Poste Italiane e il sito di compravendita e aste Ebay. Ad ogni modo si tratta sempre di soggetti che inducono un certo grado di fiducia nel destinatario.

[29] F. Cajani, G. Costabile, G. Mazzaraco, "*Phishing e furto di identità digitale – indagini informatiche e sicurezza bancaria*", 2008, Giuffré, pag. 14 e segg.

abituato[30]. Ovviamente si tratta di una pagina creata ad hoc dal *phisher*, interposta modificando i collegamenti ai server legittimi: non appena l'utente inserisce le informazioni personali, i codici d'accesso ovvero i dati relativi al proprio conto corrente, il *phisher* è in grado di recuperare dalla pagina ingannevole quelle informazioni ed è quindi libero di utilizzarle per sottrarre denaro ovvero stipulare contratti, polizze assicurative, o in generale crearsi qualsivoglia tipo di vantaggio economico. Infatti succede spesso che il *phisher* acquisisca i dati per poi rivenderli su un mercato secondario, senza provocare direttamente il danno economico alla persona successivamente offesa[31].

Successivamente alla captazione fraudolenta dei dati, sorge per il *phisher* la necessità di disperdere le tracce informatiche dei propri movimenti e soprattutto degli spostamenti di denaro: ciò avviene attraverso il reclutamento dei cc.dd. *financial manager*, preferibilmente con l'invio di altre e-mail che promettono opportunità di lavoro e/o guadagno, spesso fingendosi reali imprese alla ricerca di collaboratori. Una volta "pescato" l'utente, gli viene chiesta la disponibilità del conto corrente, a fronte di un corrispettivo che solitamente è quantificato in una percentuale delle somme depositate e poi di nuovo spostate. Le somme, spesso piuttosto elevate, dovranno solamente essere ospitate per un breve periodo e successivamente trasferite attraverso bonifici o con sistemi di money transfer (es. Western Union) su altri conti correnti o a favore di società fiduciarie, al fine di incassare finalmente il denaro frodato: così facendo si crea una catena di trasferimenti che rende piuttosto difficoltoso il lavoro degli inquirenti, facendo gradualmente perdere le tracce delle somme spostate da conto a conto, da banca a banca, coinvolgendo persone fisiche, società reali e fittizie, finché non vengono riscosse da fiduciari degli stessi truffatori oppure riescono ad evadere i controlli specifici che di regola sussistono sui bonifici

[30] Altro sistema utile per frodare informazioni a chi legge ancora messaggi in formato HTML, eliminando la necessità di azionare il collegamento internet con il browser, è presentare direttamente nel testo della e-mail una replica della pagina di login. F. Cajani, G. Costabile, G. Mazzaraco, *op.cit.*

[31] Esiste proprio un mercato nero dei dati, cui i frodatori partecipano prendendo parte a diversi forum di mediazione online, canali chat o social network. F. Cajani, G. Costabile, G. Mazzaraco, *op.cit.*

verso l'estero[32].

Oltre a quello sopra indicato come "ingannevole", realizzato con la necessaria collaborazione della vittima, il "phishing" può essere posto in essere attraverso varie modalità, fra le quali spiccano il phishing basato su *malware*, il cd. *Keylogger* o *Screenlogger* ed il phishing "*Man-in-the-middle*". Con il primo si intende quel tipo di attacco informatico realizzato mediante l'esecuzione di un software malevolo sul terminale dell'utente a sua insaputa: il programma, installato sul computer con l'inganno oppure sfruttando i *bugs* che spesso rimangono nei sistemi di sicurezza[33], entra in esecuzione in background e carpisce fraudolentemente i dati sensibili e le informazioni bancarie dell'utente, inoltrandole poi automaticamente al phisher.

I *Keylogger* (registratori di tasti) sono programmi autoinstallanti nel *browser web* o nel *driver* del dispositivo di input (per es. tastiera), al fine di osservare i dati immessi, registrarli e quindi inviare quelli di interesse ad un server già predisposto dal phisher: in questo modo viene monitorata costantemente la postazione dell'utente e può essere scoperta una grande varietà di credenziali, trasmettendo tutte – o solo – quelle che possono risultare utili per un eventuale profitto. Nell'attacco "*Man-in-the-middle*" infine il phisher si posiziona fra l'utente e il sito legittimo, ma non invia alcuna e-mail ingannevole. Egli fa in modo di intercettare i messaggi destinati in realtà al sito legittimo, conservando le informazioni di proprio interesse: dopodiché fa proseguire la comunicazione fra l'utente e il suo destinatario, inoltrando vicendevolmente le comunicazioni. Si tratta di una pratica subdola molto difficile da scoprire, poiché in apparenza il sistema di comunicazione funziona perfettamente e possono non sussistere indicazioni esteriori che fanno capire che qualcosa è stato manomesso.

Evoluzione più sofisticata del "phishing" è il cd. *Pharming*[34], più redditizio e più pericoloso poiché non implica l'invio di alcuna e-mail esca, né occorre

[32] C. del Re, "*La frode informatica*", 2009, ed. Polistampa, pag. 99; F. Cajani, G. Costabile, G. Mazzaraco, *op.cit.*

[33] Il download del programma malevolo può essere indotto con l'inganno da parte del phisher, convincendo l'utente ad aprire un allegato nella e-mail oppure a scaricare un programma da un sito web. La diffusione può avvenire anche attraverso *security exploits* (attacchi alla sicurezza) realizzati spesso con la diffusione di worm o virus. F. Cajani, G. Costabile, G. Mazzaraco, *op.cit.*

[34] Il termine fu coniato per la prima volta dal *Sans Institute System administration, networking and security*: http://www.sans.org/

convincere in qualche modo l'utente a visitare siti fasulli: si tratta di una tecnica di cracking sempre volta ad ottenere l'accesso ad informazioni personali e riservate, ma inducendo inconsapevolmente l'utente stesso a riverlarle. L'agente dapprima altera il sistema di connessione con il server web che fornisce l'indirizzo IP del sito web vittima dell'attacco, poi crea una pagina replica dello stesso, che verrà utilizzata come server per la "pesca" di dati. L'obiettivo primario è il server DNS dell'Internet Service Provider: in altri termini, con sofisticate tecniche di cracking, viene modificato l'abbinamento fra il server che fornisce il dominio e l'indirizzo IP corrispondente. In questo modo l'utente, nel momento in cui digita l'indirizzo internet del sito subdolamente attaccato, verrà dirottato – a causa della compromissione della connessione – tramite il server trappola sul sito replica creato dal phisher, che riproduce quasi perfettamente quello originale[35]. Il computer è quindi "ingannato" dal *Domain System Name* compromesso e l'utente rivela informazioni sensibili senza porsi alcuna domanda, credendo di essere sul sito legittimo: in realtà le informazioni confluiscono direttamente nel *data-base* del phisher, il quale poi sarà libero di utilizzarle al fine di conseguire un vantaggio indebito[36]. La pericolosità di questi attacchi risiede soprattutto nel fatto che spesso non sussistono modifiche visibili agli occhi dell'utente, sia che venga infettato direttamente l'elaboratore target, sia che venga attaccato il sistema di connessioni; inoltre l'evidenza dell'attacco può essere rimossa facilmente, ripristinando le connessioni DSN legittime ovvero rimuovendo il malware responsabile della captazione dei dati.

A fronte di tale varietà di forme, bisogna preventivamente segnalare come in Italia non esista una disciplina giuridica specifica atta a sanzionare il fenomeno in discorso: il nostro ordinamento non solo non fornisce una definizione legislativa di "phishing"[37] ma altresì non punisce esplicitamente detta attività

[35] Il sito replica di solito presenta lievi imperfezioni che lo rendono identificabile come falso, ad esempio differenze di lingua nella medesima pagina, errori grammaticali, indirizzi e-mail che non contengono riferimenti al sito legittimo o cromie non esattamente coincidenti con quelle originali. Tuttavia si tratta di differenze di solito non immediatamente percepibili: perciò l'utente magari poco avvezzo all'utilizzo della rete non se ne accorge.

[36] Il *pharming* può essere altresì posto in essere direttamente ingannando il computer locale della vittima, con l'ausilio di programmi *trojan*, *malware* vari o tramite altro accesso diretto, ovvero infettando i *router* casalinghi usati per connettersi alla rete ADSL.

[37] I contributi più importanti si rinvengono negli apporti giurisprudenziali, sia di merito sia di legittimità, dove si può trovare un'interessante definizione del fenomeno: gli ermellini hanno

come unica condotta illecita, seppur complessa. Perciò è necessario individuare quali fattispecie, debitamente adattate, possano essere applicate in ciascuna delle fasi in cui si manifesta la condotta illecita.

La prima fase in cui si articola il tipico "phishing attack" si sostanzia solitamente in una qualche forma di "*identity theft*", ovvero "furto di dati identificativi", fraudolentemente raccolti e poi illecitamente utilizzati: la tutela penale apprestata all'identità personale dal nostro ordinamento è data dalla fattispecie di cui all'art. 494 c.p., considerata dalla giurisprudenza di legittimità applicabile anche qualora il predetto reato venisse commesso sulla rete Internet[38].

Il delitto di sostituzione di persona ha trovato perciò applicazione con riferimento a varie fattispecie concrete in costante aumento: si pensi alla creazione ex novo di pagine web che vengono disconosciute dai legittimi proprietari (soprattutto all'interno dei c.d. social network) recanti dati personali, informazioni sensibili ed immagini di soggetti i quali non avevano dato alcun permesso alla pubblicazione; ovvero, a casi di acquisizione indebita dell'account personale e/o profilo di Facebook (o di altre piattaforme di social network), rapportabili tra l'altro ad una condotta preliminare e qualificabile quale accesso abusivo al sistema informatico dell'utente ai sensi dell'art. 615-ter c.p.

Nonostante la positività dei risultati raggiunti, la fattispecie in discorso ha dato vita ad un vivace dibattito in dottrina, parte della quale ha mostrato di non

---

definito il phishing come "*quell'attività illecita in base alla quale, attraverso vari stratagemmi (o attraverso fasulli messaggi di posta elettronica, o attraverso veri e propri programmi informatici e malware) un soggetto riesce ad impossessarsi fraudolentemente dei codici elettronici (user e password) di un utente, codici che, poi, utilizza per frodi informatiche consistenti, di solito, nell'accedere a conti correnti bancari o postali che vengono rapidamente svuotati*". Cass. Pen., sez. II, sent. n. 9891 del 11/03/2011.

[38] Cass. Pen., sez. IV, sent. n. 25774 del 11/07/2014; Cass. Pen., Sez. V, sent. n. 46674 del 9/11/2007. In tale sentenza, la Corte di Cassazione aveva già mostrato di non considerare d'ostacolo all'applicazione della fattispecie di cui all'art. 494 c.p. lo strumento informatico, ritenendo sussistente invece la lesione alla pubblica fede in quanto le informazioni diffuse in Internet possono raggiungere una platea vastissima di soggetti: "*oggetto della tutela penale è l'interesse riguardante la pubblica fede, in quanto questa può essere sorpresa da inganni relativi alla vera essenza di una persona o alla sua identità o ai suoi attributi sociali. E siccome si tratta di inganni che possono superare la ristretta cerchia d'un determinato destinatario, così il legislatore ha ravvisato in essi una costante insidia alla fede pubblica, e non soltanto alla fede privata e alla tutela civilistica del diritto al nome*". Così poi prosegue la sentenza: "*nel caso in esame il soggetto indotto in errore non è tanto l'ente fornitore del servizio di posta elettronica, quanto piuttosto gli utenti della rete, i quali, ritenendo di interloquire con una determinata persona (la T.), in realtà inconsapevolmente si sono trovati ad avere a che fare con una persona diversa*".

condividerne l'applicazione al fenomeno "phishing" a causa di alcuni ostacoli interpretativi ritenuti insormontabili: in primis si è rilevato come l'invio di una e-mail atta ad imitare pedissequamente il "*look and feel*" di loghi e siti di mittenti reali, non significhi che il riferimento indichi o distingua un mittente come "persona fisica", perciò non può configurarsi la sostituzione di una persona ad un'altra; l'uso on-line degli estremi identificativi di una persona reale, come le credenziali di autenticazione per l'accesso a sistemi informatici o spazi virtuali esclusivi, non corrisponde all'attribuzione tipizzata di un "falso nome", un "falso stato", o una "qualità a cui la legge attribuisce effetti giuridici", dato che non viene affatto utilizzato un dato intrinsecamente falso, bensì è il soggetto corrispondente al dato ad essere differente; infine, insormontabile è apparso a costoro l'ostacolo dell'evento consumativo, essendo "l'induzione in errore" di taluno totalmente incompatibile od inapplicabile all'esecuzione automatizzata di richieste inoltrate a sistemi informatici. Il fatto che la condotta si rivolga in prima battuta all'elaboratore elettronico rimane il *punctum dolens*: non è possibile sostenere che l'inserimento on-line di dati o delle credenziali del soggetto passivo da parte dell'agente tragga in inganno il sistema informatico, poiché quest'ultimo esegue unicamente le istruzioni impartitegli dalla persona fisica che lo utilizza, che per esso corrisponde a quella legittimata, in quanto utilizzatore dell'"identità virtuale"[39].

Altra dottrina ha sostenuto come a ben vedere, si tratti di opinioni critiche potenzialmente aggirabili ai fini dell'applicazione della norma in esame alle fattispecie indicate, spostando il focus dell'attenzione dall'elaboratore elettronico alla persona fisica effettivamente tratta in inganno. Considerando il sistema informatico semplicemente come strumento dell'attività illecita, in quanto tale astrattamente sostituibile con una missiva cartacea, una telefonata, o qualsiasi altro espediente, è evidente come l'evento consumativo del reato di sostituzione di persona sia a tutti gli effetti sussistente: l'agente trae in inganno, a mezzo di una messaggio inviato per posta elettronica, l'ignaro utente di Internet, sostituendosi al legittimo mittente proprio grazie all'utilizzo fraudolento

[39] R. Flor, "*Phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*", Riv. it. dir. e proc. pen., fasc. 2-3, 2007, p. 899.

dei suoi elementi distintivi, quali il logo, il marchio, lo stile e i colori di scrittura, il nome. Perciò si può ritenere sussistente la prima condotta tipizzata all'art. 494 c.p., ovvero "*l'induzione di taluno in errore, sostituendo illegittimamente la propria all'altrui persona*": non è necessario che siano integrati anche gli estremi della seconda condotta tipica, ovvero "l'attribuzione di un dato falso", essendo la disposizione composta di due condotte a tutti gli effetti indipendenti e autonomamente rilevabili.

Anche così argomentando, tuttavia, permangono alcune perplessità in ordine all'elemento soggettivo, dato che nel caso di "phishing" – di regola – l'agente non pone in essere la condotta con il fine precipuo di ingannare la persona offesa: lo scopo primario che guida l'azione è il vantaggio patrimoniale che può derivare dall'utilizzo in prima persona o dallo sfruttamento commerciale dei dati, perciò l'inganno della vittima è un "male collaterale necessario", come avviene nell'ipotesi di furto aggravato dall'impiego di mezzi fraudolenti.

Da parte sua, la giurisprudenza più recente, attenta agli aspetti sostanzialistici dell'interpretazione e agli effetti concreti in termini di tutela da apprestare al caso sottoposto al proprio vaglio, non ha avuto dubbi nell'applicare la fattispecie di cui all'art. 494 c.p. ai casi di "phishing", ritenendo integrati gli estremi del reato di sostituzione di persona in quella che possiamo considerare la fase 1 dell'attacco, vale a dire il momento d'invio di messaggi di posta elettronica in apparenza proveniente da un mittente legittimo attraverso i quali viene realizzata la "raccolta" o "pesca" di dati riservati dell'utente[40].

Per quanto attiene specificamente alla seconda fase d'attacco, ossia al momento di utilizzo dei dati fraudolentemente carpiti per realizzare un illecito profitto a mezzo di operazioni on-line, il panorama giurisprudenziale è piuttosto variegato: molti giudici di merito si sono orientati verso l'applicazione in concorso dei reati di accesso abusivo al sistema informatico (art. 615-ter c.p.) e truffa (art. 640 c.p.)[41]: se la sussistenza del primo delitto non desta alcun

[40] Trib. Milano, 7 ottobre 2011, Pres. Pellegrino Est. Corbetta.

[41] Trib. Milano, 7 ottobre 2011, Pres. Pellegrino, Est. Corbetta: "*chi, avvalendosi delle tecniche del c.d. phishing, mediante artifici e raggiri realizzati attraverso l'invio di false e-mail e la creazione di false pagine web in tutto simili a quelle di primari Istituti di Credito, dopo aver indotto in errore l'utente ed essersi fatto rivelare le credenziali di accesso, si introduca nel servizio di home banking della vittima per effettuare operazioni di prelievo o bonifico on-line non*

dubbio, essendo pacifico che "*l'illecita introduzione nel sistema informatico delle banche attraverso i dati, illecitamente acquisti, relativi al conto corrente delle vittime che cadono nella trappola, integra il delitto ex art. 615-ter c.p.*", qualche perplessità suscita la ritenuta sussistenza del delitto di cui all'art. 640 c.p. nel caso di utilizzo dei dati altrui raccolti con l'inganno per realizzare operazioni nella rete internet.

Nelle (poche) sentenze che affrontano il fenomeno in esame nel suo complesso, l'argomentazione sul punto risulta poco solida dal punto di vista tecnico e induce a tratti confusione: spesso si sono ravvisati gli "artifici e raggiri" di cui all'art. 640 c.p. in un elemento tipico fondamentale del reato di cui all'art. 494 c.p. (l'invio di e-mail false o la creazione di false pagine web) contestato in concorso per punire la condotta della c.d. fase 1. Ne deriva qualche frizione con il principio del *ne bis in idem sostanziale*, che fa divieto di attribuire due volte ad un medesimo autore un accadimento unitariamente valutabile dal punto di vista normativo[42]: in tal caso il disvalore della condotta di adescamento è già pienamente assorbito dal delitto di sostituzione di persona. In un altro caso meno recente si è tentato di evitare di incorrere in una duplice sanzione del medesimo comportamento materiale contestando solo il delitto di truffa: il giudice ha ravvisato gli estremi dell'induzione in errore del soggetto passivo nella condotta di riproduzione di siti web che costituiscono interlocutori abituali dell'utente medio dei servizi on-line, mentre gli artifici e raggiri sono stati individuati nell'utilizzo di e-mail intestate dove sono riprodotti colori, marchi ed altre caratteristiche che si rinvengono nelle normali delle modalità di interazione tra soggetto passivo ed interlocutore legittimo[43]. Tale soluzione, basata su un'interpretazione meramente letterale di quanto disposto dall'art. 640 c.p., si scontra con la dottrina maggioritaria in tema di truffa, la quale sostiene come sia necessario che l'atto di disposizione patrimoniale prodromico alla realizzazione

---

autorizzate risponde dei delitti di sostituzione di persona (art. 494 c.p.), accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.), truffa (art. 640 c.p.)"

[42] G. Fiandaca, E. Musco, "*Diritto penale – Parte generale*", sesta ed., Zanichelli, 2009.

[43] "*Integra il delitto di truffa, e non quello di frode informatica, il conseguimento di un ingiusto profitto ottenuto attraverso l'invio di e-mail contraffatte nel mittente e tramite siti civetta (c.d. phishing) finalizzato al conseguimento di credenziali per il dirottamento dei fondi degli utenti di siti di home banking su carte prepagate o conti nella disponibilità di un'organizzazione criminale*", in Trib. Milano, 10/12/2007 (sent.), G.I.P. Gamacchio.

dell'evento dannoso sia compiuto dalla stessa persona che è stata indotta in errore: non è possibile che lo spostamento patrimoniale sia posto in essere dal truffatore. In effetti la norma sul punto non è affatto chiara, perciò la soluzione prospettata dal giudice del Tribunale di Milano è astrattamente ammissibile, pur ponendosi in contrasto con il ritenuto assetto tradizionale della truffa.

Da quanto esposto, si può desumere la diversificazione delle argomentazioni fornite dalla giurisprudenza sul punto, le quali si dimostrano ondivaghe e spesso non sono nemmeno particolarmente limpide, a testimonianza altresì della scarsa conoscenza informatica del fenomeno e della conseguente difficoltà di inquadramento giuridico.

Anche la dottrina, nel tentativo di rinvenire nell'ordinamento una fattispecie legale adatta a queste condotte, si è interrogata a lungo circa la possibilità di applicazione del reato di cui all'art. 640 c.p. ovvero del reato di cui all'art. 640-ter c.p.. In un primo momento, tramite l'isolata analisi della materialità delle condotte dei primi attacchi di "phishing", è prevalsa la tesi della configurabilità della truffa. Questo orientamento ermeneutico, infatti, evidenziava come non si potessero ritenere sussistenti gli elementi tipici del delitto di frode informatica nel fenomeno in esame, poiché l'attacco si sostanziava nell'utilizzo di artifizi o raggiri verso una persona fisica, cui seguiva la *deminutio patrimonii*: non si concretizzava né la condotta di "*alterazione del funzionamento di un sistema informatico*" né quella di "*intervento senza diritto su dati, informazioni o programmi contenuti in tale sistema*".

Più recentemente, invece, un opposto orientamento dottrinale – avallato altresì dalla giurisprudenza di legittimità – è giunto ad accogliere una diversa impostazione più tecnica, atta a valorizzare il momento dell'utilizzo delle credenziali indebitamente acquisite: si è compreso come in molti attacchi di "phishing" sussista l'alterazione del funzionamento del sistema informatico, effettuata mediante l'installazione fraudolenta sul PC della vittima di software malevoli o cavalli di Troia, ovvero sussista l'"intervento non autorizzato su dati o informazioni" del correntista, nel caso di trasferimenti di fondi tramite l'home-banking. Proprio come testualmente prevede l'art. 640-ter c.p.[44].

[44] In tal senso vedi Cass. Pen., sez. II, sent. n. 9891 del 24/02/2011.

A ben vedere, una volta contestata la sostituzione di persona, la residua condotta può astrattamente assumere sia la forma della frode informatica sia quella della truffa; e non si esclude che possano altresì concretizzarsi le fattispecie di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.), nell'ipotesi di reperimento, riproduzione, diffusione, comunicazione, consegna ad altri di codici di accesso o di indicazioni utili con fine di profitto ovvero di indebito utilizzo di carte di credito e di pagamento su Internet, al ricorrere dei presupposti indicati dall'art. 55 c. IX D.lgs. 231/2007: è necessario condurre un'attenta analisi delle concrete modalità operative dell'azione, poiché la contestazione dipenderà da come nei fatti avviene la *deminutio patrimonii* da parte del soggetto agente con correlativo vantaggio ingiusto per sé o altri. Se questi utilizza sempre il sistema informatico o telematico, ponendo in essere una condotta di "*alterazione in qualsiasi modo*" dello stesso, ad esempio con l'installazione fraudolenta di un *malware* o di un *Trojan horse* in grado di funzionare in background e carpire in tal modo i dati, ovvero "*intervenendo senza diritto su dati, informazioni o programmi contenuti in un sistema informatico o telematico*", ad esempio effettuando, successivamente alla captazione fraudolenta delle informazioni altrui, operazioni di home banking o acquisti on-line, non v'è dubbio che sussisteranno gli estremi del delitto di frode informatica.

È necessario perciò condurre un'attenta analisi sulle modalità attraverso le quali viene posta in essere la condotta di "phishing" da parte del soggetto agente: per contestare la fattispecie di frode informatica deve sussistere, nel caso della prima condotta tipica, una effettiva manipolazione dell'elaboratore o del sistema telematico che permetta all'agente di captare quei dati sensibili necessari ad ottenere il vantaggio patrimoniale indebito, causando il danno ingiusto. Nel caso della seconda condotta invece, la contestazione avverrà tendenzialmente in concorso con il delitto di sostituzione di persona (art. 494 c.p.), poiché l'agente interviene in maniera abusiva su un sistema informatico o telematico sfruttando illegittimamente quei dati personali "pescati" attraverso l'invio di e-mail copia o la creazione di siti web "spoofed" (imitazioni): l'azione, in apparenza del tutto regolare, risulta illecita ai sensi della normativa penale solamente per il fatto che

viene realizzata da colui il quale non è stato in alcun modo legittimato, né dall'amministratore del sistema violato, né dal titolare dei dati frodati, avvenendo perciò "senza diritto", *id est* senza alcuna facoltà legittima.

Non può essere escluso a priori che si realizzino gli estremi del delitto di truffa ex art. 640 c.p.: sarà una contestazione caratterizzata da uno spazio d'intervento spesso residuale, essendo riscontrabile nelle ipotesi di *deminutio patrimonii – id est*, operazioni sui conti correnti delle ignare vittime – realizzate con artifizi e raggiri ma senza manipolare o intervenire in maniera non autorizzata su un sistema informatico o telematico[45].

La configurazione in termini giuridici della fattispecie successiva all'indebita captazione di dati potrà assumere la forma persino dell'indebito utilizzo di carte di credito o pagamento, se l'agente dovesse porre in essere una delle condotte tipizzate all'art. 55, c. IX D.lgs. 231/2007, ossia da un lato utilizzare i dati inerenti agli strumenti di pagamento per acquistare senza alcuna legittima facoltà beni o servizi ovvero indebitare la posizione dell'ignaro titolare della carta, dall'altro sfruttare gli stessi dati per creare – e o cedere, possedere o acquisire – carte di credito o debito falsificate.

Con l'entrata in vigore del D.lg. n. 93 del 14/08/2013 il panorama normativo si è arricchito della nuova aggravante ad effetto speciale collocata al terzo comma dell'art. 640-ter c.p. che sanziona più gravemente rispetto all'ipotesi base la frode informatica commessa con "*furto o indebito utilizzo di identità digitale*": si tratta di un'integrazione voluta dal legislatore proprio per dimostrare maggior attenzione e protezione in favore delle sempre più numerose vittime di furti di dati sensibili on-line al fine di ottenere vantaggi patrimoniali ingiusti.

La nuova previsione normativa sembra infatti creata a misura di "phishing", almeno nei casi in cui avvenga attraverso una manipolazione dei dati nell'elaboratore, mantenendo il focus della repressione penale sulla condotta

[45] Trib. Milano, 7 ottobre 2011 (sent.), Pres. Pellegrino Est. Corbetta. Dopo aver argomentato la contestazione dei delitti di cui all'art. 494 c.p. e art. 615-ter c.p., i giudici così proseguono: "*il phisher si rende responsabile anche del delitto di truffa, di cui ricorrono tutti gli elementi costitutivi: l'artificio o il raggiro, consistente, appunto, nell'invio di false e-mail e nella creazione di false pagine web; l'errore in cui cade il destinatario della mail, il quale ritiene provengano dalla banca di cui è cliente, così fornendo inconsapevolmente i dati di accesso del proprio conto corrente; l'ingiusto profitto con correlativo altrui danno, rappresentato dalle somme di denaro illecitamente sottratte dal conto corrente della vittima*".

cui è finalizzata la stessa sottrazione delle informazioni: in altri termini, la contestazione da parte della giurisprudenza maggioritaria del delitto di cui all'art. 494 c.p. per sanzionare la cd. "fase 1" del fenomeno in parola ha avuto il pregio di sfruttare le norme a disposizione per punire una condotta, considerata pacificamente offensiva, che altrimenti avrebbe corso il rischio di rimanere priva di presidio penalistico, ma ha destato qualche – fondata – perplessità soprattutto per la difficoltà, spesso, di rinvenire l'evento intermedio dell'"induzione in errore". L'alternativa era la contestazione del solo delitto di truffa, snaturandolo però rispetto alla configurazione fattuale tradizionale e non rispondendo pienamente alla pericolosità della condotta informatica.

L'invio massiccio di e-mail *spam*, il confezionamento di *malware* o *Trojan horses* atti al recupero surrettizio di dati dall'elaboratore della vittima, la creazione di siti web "*spoofed*" quali server per il "phishing" sono tutte condotte che permettono al phisher il "*furto o indebito utilizzo di identità digitale in danno di uno o più soggetti*"[46] e sono strumentali alla realizzazione del profitto derivante dal depauperamento del patrimonio altrui.

È evidente come ciò permetta una contestazione più aderente alla fenomenologia dell'offesa e una risposta sanzionatoria più rispondente al disvalore della condotta: non si tratta di due fattispecie indipendenti commesse in concorso, né di una semplice ipotesi di truffa, bensì di un'offesa ad un unico bene giuridico, un unico reato posto in essere attraverso una modalità particolarmente insidiosa, che richiede un maggior rigore punitivo.

La vicinanza alla struttura della fattispecie aggravata prevista all'art. 625 comma 1 n. 2 c.p. è notevole: per mezzo fraudolento si intende uno strumento oppure uno stratagemma diretto a superare l'ostacolo che l'avente diritto abbia posto a difesa del bene. Le parole utilizzate dai giudici di legittimità per descrivere questa particolare modalità di condotta si adattano altresì alla "pesca dei dati" con l'inganno: la condotta, posta in essere nel corso dell'iter criminoso, è "*dotata di marcata efficienza offensiva e caratterizzata da insidiosità, astuzia,*

[46] Interpretando il concetto di identità digitale in senso lato come qualsiasi insieme di informazioni, credenziali o dati reperibili in un sistema informatico o telematico utili ad individuare nello stesso un'unica persona fisica, quale titolare legittimo degli stessi. Per un approfondimento si rinvia al cap. III par. 2.

scaltrezza, volta a sorprendere la contraria volontà del detentore ed a vanificare le difese che questi ha apprestato a difesa del possesso della cosa"[47].

La contestazione ai sensi dell'art. 640-ter c.p. alla luce del nuovo comma 3 comporta evidenti i vantaggi sia di natura procedimentale sia di natura sostanziale, quali la possibilità di concentrare le indagini e la ricerca delle prove su un'unica fattispecie delittuosa e quindi un unico evento di reato, la procedibilità ex officio e dei limiti edittali più elevati rispetto al delitto di truffa (art. 640 c.p.), che rispondono maggiormente alla intrinseca gravità dello strumento d'offesa.

Il delitto di sostituzione di persona (art. 494 c.p.) potrà trovare applicazione residuale in tutti quei casi in cui la sottrazione o l'utilizzo fraudolento di informazioni altrui avvenga al fine di procurare a sé o ad altri un vantaggio di qualsiasi natura[48], recando contemporaneamente offesa alla fede pubblica: questa può essere sorpresa da inganni relativi alla vera essenza di una persona o alla sua identità o ai suoi attributi sociali. Siccome si tratta di inganni che possono superare la ristretta cerchia di un determinato destinatario, il legislatore ha ravvisato in essi una costante minaccia alla fede pubblica, e non soltanto alla fede privata e alla tutela civilistica del diritto al nome[49]. La Corte di Cassazione ha ritenuto infatti che si configuri il delitto di sostituzione di persona nella condotta di colui che crei ed utilizzi un "account" ed una casella di posta elettronica, servendosi dei dati anagrafici di un diverso soggetto, inconsapevole, con il fine di far ricadere su quest'ultimo l'inadempimento delle obbligazioni conseguenti all'avvenuto acquisto di beni mediante la partecipazione ad aste in rete[50] ovvero crei o utilizzi un determinato profilo su un social network riproducente l'immagine della persona offesa, con una descrizione tutt'altro che lusinghiera e grazie alla stessa usufruisce dei servizi del sito, consistenti

[47] Cass., Sez. Unite, sent. n. 40354 del 18/07/2013 (dep. 30/09/2013)

[48] Nell'art. 494 c.p. il legislatore sceglie di utilizzare la dizione "*procurare a sé o ad altri un vantaggio*", non un profitto, a testimonianza della differenza concettuale sottesa alle due espressioni. L'utilizzo del termine "vantaggio" infatti amplia notevolmente i confini della fattispecie, rendendola applicabile a tutte quelle ipotesi in cui l'agente ottenga dalla propria condotta illecita un beneficio di qualsiasi natura, non necessariamente patrimoniale.
L'utilizzo del termine "profitto" nella fattispecie di cui all'art. 640-ter c.p. conferisce alla stessa una connotazione prettamente patrimoniale.

[49] Cass. Pen., sez. IV, sent. n. 25774 del 16/06/2014.

[50] Cass. Pen., sez. III, sent. n. 12479 del 15/12/2011 (dep. 3/04/2012)

essenzialmente nella possibilità di comunicazione in rete con altri iscritti e di condivisione di contenuti[51]: l'evento di induzione in errore e il dolo specifico di ottenere un qualsiasi tipo di vantaggio causando danno ad altri sono pienamente sussistenti. Al contempo, non sussistono gli elementi tipici essenziali per ritenere sussistente una frode informatica, vale a dire in primis l'indebito spostamento patrimoniale derivante da una manipolazione informatica, cui consegua un profitto per l'agente e una *locupletatio iniusta* per la persona offesa.

Passando a quella che possiamo definire la "fase 2" del *phishing-attack*, si registrano – allo stato – ancora alcuni problemi irrisolti circa l'inquadramento giuridico del *financial manager.* L'esperienza delle Procure Distrettuali ha rivelato come, nella maggior parte dei casi di "phishing" indagati, siano presenti sul territorio italiano soggetti compiacenti che attivano appositamente delle carte di pagamento ricaricabili, previa comunicazione dei relativi dati identificativi al phisher o a chi collabora con esso, rendendosi disponibili a prelevare in contanti le somme di denaro fatte confluire su tali strumenti elettronici attraverso trasferimenti online[52]. Il denaro, detratta una percentuale a titolo di ricompensa, viene poi trasferito all'estero tramite il sistema Western Union o Money Gram, canali idonei ad interrompere la tracciabilità dei flussi monetari.

Il dibattito giurisprudenziale verte sulla configurabilità in capo a tali soggetti di una responsabilità a titolo di concorso nei reati presupposto ovvero di una responsabilità per i delitti di ricettazione o riciclaggio. I problemi applicativi derivano dal fatto che spesso è del tutto evidente l'assenza di un dolo intenzionale o diretto di riciclaggio, perciò si è dibattuto sulla compatibilità della fattispecie di cui all'art. 648-bis c.p. con il dolo eventuale e, se del caso, sulla possibilità di contestare il delitto di ricettazione ex art. 648 c.p..

La più recente giurisprudenza ha chiarito come il *financial manager* risponda a

[51] Cass. Pen., sez. IV, sent. n. 25774 del 16/06/2014; Cass. Pen., sez. V, sent. n. 18826 del 28/11/2012; Cass. Pen., sez. V, sent. n. 46674 del 08/11/2007.

[52] Spesso Le indagini si concludono solo con l'individuazione proprio del *financial manager*, l'ultimo anello di una catena ben più lunga e articolata, rispetto alla quale l'identificazione dei phisher (il più delle volte operanti all'estero) e soprattutto la loro condanna appare difficoltosa.

titolo di concorso nei medesimi delitti realizzati dal phisher solo se ha agito con la piena consapevolezza della complessiva attività fraudolenta posta in essere a danno dei correntisti e del suo ruolo all'interno della stessa: è necessario perciò che sussistano elementi di prova specifici, idonei a dimostrare che il ritenuto *financial manager* abbia contribuito personalmente e direttamente – in concorso con altri – alla complessiva attività fraudolenta di carattere informatico, oppure che lo stesso abbia apportato il proprio contributo morale, ossia di istigazione o di rafforzamento dell'altrui proposito criminoso[53].

Tale soggetto deve essere pienamente consapevole del fatto che proprio la sua collaborazione – che si sostanzia nel trasferimento online sulla sua carta ricaricabile del denaro e del successivo passaggio all'estero – permette la piena realizzazione del progetto criminoso del phisher, rendendo difficile, se non impossibile, rintracciare le somme frodate[54].

Se, invece, rimane del tutto ignaro del disegno criminoso complessivo[55], può rispondere di delitti di ricettazione (art. 648 c.p.) o di riciclaggio (art. 648-bis c.p.), a seconda che si sia limitato a ricevere le somme di denaro, con la consapevolezza della loro provenienza illecita, ovvero le abbia altresì trasferite all'estero con modalità idonee ad ostacolare l'identificazione di tale provenienza. L'affermazione della responsabilità per il delitto di ricettazione è autonoma rispetto all'accertamento degli elementi costitutivi del reato presupposto e si basa sulla valutazione degli elementi concreti noti all'agente: non richiede pertanto l'accertamento giudiziale del delitto che ne costituisce il presupposto (ossia il "phishing"), né dei suoi autori, né dell'esatta tipologia del reato, essendo sufficiente che il giudice acclari l'esistenza di un fatto illecito attraverso prove logiche[56].

---

[53] Trib. Milano, Giudice per le indagini preliminari – sent. 2507 del 10/04/2013 (est. Ferraro)

[54] S. Piancastelli, "*La ricezione di somme di denaro provento di phishing: risultanze investigative e problemi applicativi in punto di qualificazione giuridica - Nota a Trib. Milano, uff. g.i.p., sent. 10/04/2013, n. 2507, giud. Ferraro, imp. Ciavarella e Trib. Milano, sez. VI penale, sent. 28/05/2013, n. 6753, giud. Bernazzani, imp. Trozzola*", 3 marzo 2015, articolo reperibile su www.penalecontemporaneo.it

[55] Di regola le fattispecie astratte finora più contestate sono la sostituzione di persona (art. 494 c.p.), l'accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.) e la frode informatica (art. 640-ter c.p.).

[56] Trib. Milano, sez. VI penale in composizione monocratica – sent. 6753/2013 (est. Bernazzani); S. Piancastelli, *op.cit*.; S. Battaglia, "*Criminalità informatica al tempo di internet: rapporti tra phishing e riciclaggio*", articolo del 18/09/2013 reperibile su www.altalex.com

Il dolo di ricettazione o riciclaggio può dirsi sussistente in capo al *financial manager* solo quando, sulla base di precisi elementi di fatto, si possa affermare che questi si sia seriamente rappresentato l'eventualità della provenienza delittuosa del denaro e, cionondimeno, abbia comunque deciso di riceverlo e trasferirlo all'estero con le modalità indicate dal phisher[57]. In termini soggettivi ciò significa che non può rinvenirsi nel mero sospetto della provenienza illecita del denaro: deve trattarsi di un atteggiamento psicologico inequivoco che, pur non attingendo il livello della certezza, implica da parte dell'agente la necessità di compiere una scelta consapevole tra l'agire, rappresentandosi la concreta possibilità della provenienza della cosa da delitto, e il non agire[58].
In conclusione, l'affermazione di una responsabilità a titolo di concorso nei reati di frode informatica ed accesso abusivo, piuttosto che per il reato di ricettazione, corre sul sottile crinale che si colloca tra la previa piena consapevolezza, in capo all'imputato, dell'intero e specifico *modus operandi* e la semplice generica consapevolezza della illiceità dell'operazione precedente.

Una volta che risulti appurato, o comunque non sia più oggetto di contestazione, l'avvenuto raggiro dei correntisti ad opera di uno scaltro phisher, si pone una rilevante questione di natura civilistica, relativa alla possibilità o meno di individuare un profilo di responsabilità – a titolo contrattuale ovvero extracontrattuale – in capo all'intermediario che fornisce ai suoi clienti l'utilizzo di servizi *online*: in altri termini, è necessario capire se costui sia tenuto a rifondere il pregiudizio patito dai propri clienti o se non altro a ripianare

[57] Cass. sez. Unite, sent. n. 12433 del 26/11/2009; i giudici hanno considerato compatibile il dolo eventuale con il delitto di ricettazione, escludendo tuttavia il mero sospetto dalla latitudine di tale stato psicologico, osservando che: "*fermo rimanendo quindi che la ricettazione può essere sorretta anche da un dolo eventuale resta da stabilire come debba avvenire il suo accertamento e quali debbano essere le sue caratteristiche, posto che lo stesso non può desumersi da semplici motivi di sospetto e non può consistere in un mero sospetto, se è vero che questo non è incompatibile con l'incauto acquisto. Occorrono per la ricettazione circostanze più consistenti di quelle che danno semplicemente motivo di sospettare che la cosa provenga da delitto, sicché un ragionevole convincimento che l'agente ha consapevolmente accettato il rischio della provenienza delittuosa può trarsi solo dalla presenza di dati di fatto inequivoci, che rendano palese la concreta possibilità di una tale provenienza*"; Cass. Pen., sez. II, sent. n. 25960 del 17/06/2011

[58] In Cass. Pen., sez. II, sent. n. 2436 del 27/02/1997 la Corte si è spinta ad affermare che "*la prova del dolo può essere desunta da qualsiasi elemento, anche indiretto, e la stessa mancata o non attendibile giustificazione del possesso di una cosa proveniente da delitto costituisce prova della conoscenza dell'illecita provenienza del bene*".

parzialmente la perdita.

È frequente rinvenire nei contratti che regolano i servizi bancari, al fine di poter successivamente radicare la responsabilità in capo al correntista nel caso di movimentazioni bancarie non riconducibili allo stesso, clausole che prevedono specificamente l'obbligo per lo stesso di conservare con cura le credenziali fornite dall'intermediario: violando dette previsioni, il cliente si espone alla responsabilità *ex contractu* per ogni effetto che possa scaturire dall'abuso o dall'uso illecito delle stesse. Dato che è comunque da escludere la possibilità di attribuire preventivamente ed esclusivamente la responsabilità al correntista, essendo necessario altresì un accertamento relativo alla condotta tenuta dalla controparte contrattuale, il punto nevralgico della questione consiste nel valutare se la condotta incauta del cliente sia o meno prevalente rispetto alla diligenza professionale sempre richiesta all'intermediario. Tale soggetto, infatti, nel fornire servizi telematici, ha l'obbligo di adottare tutte le cautele e gli accorgimenti idonei, in base al criterio della diligenza professionale previsto dal codice civile, ad evitare conseguenze dannose, nonché a prevenire e impedire la produzione di effetti ulteriori rispetto alla frode informatica.

Si hanno quindi due differenti poli verso i quali la responsabilità può astrattamente tendere e la giurisprudenza, assieme agli organismi indipendenti che si occupano di dirimere le controversie bancarie[59], sono stati negli anni a lungo divisi, fornendo differenti valutazioni ed argomentazioni sul tema.

La prima tendenza giurisprudenziale è stata quella di risolvere la questione nel senso più favorevole al soggetto intermediario, utilizzando le disposizioni relative alla responsabilità contrattuale contenute nel codice civile: si sono registrate infatti uniformi decisioni da parte del Tribunale di Milano nel 2006, del Giudice di Pace di Lecce e del Giudice di Pace di Badolado nel 2008, nelle quali si è stabilita la responsabilità piena del correntista, in assenza di prova certa che riferisse i fatti frode alla responsabilità dell'istituto di credito, per

[59] L'art. 128-bis del Testo Unico Bancario ha introdotto nel nostro ordinamento la figura dell'Arbitro Bancario Finanziario, organismo indipendente ed imparziale, operativo dall'estate del 2009, che si occupa della risoluzione in via stragiudiziale delle controversie che possono insorgere fra gli istituti di credito e i loro clienti. Si tratta di un'alternativa celere e poco costosa (non prevedendo la necessità di assistenza legale) al giudizio ordinario: le sue decisioni tuttavia non sono vincolanti e, se le parti non sono soddisfatte, possono rivolgersi al giudice ordinario.

presunta violazione delle norme contrattuali[60]. In altri termini, non sussistendo l'evidenza probatoria del nesso causale fra l'avvenuta frode e la supposta inadeguatezza delle misure di sicurezza del sistema informatico, l'intermediario non avrebbe dovuto rispondere del danno patito dal proprio cliente, il quale era ritenuto unico responsabile per non aver utilizzato la carta di pagamento in maniera oculata e prudente.

Nel 2010, con le prime pronunce dell'Arbitro Bancario Finanziario e l'introduzione della disciplina sui servizi di pagamento[61], ha iniziato ad affermarsi un orientamento più favorevole ai correntisti: in una delle prime decisioni[62] resa dal Collegio di Milano si è ravvisato un concorso di colpa tra la banca, per violazione dell'obbligo di diligente custodia dei patrimoni dei clienti, ed il correntista, per incauta custodia dei codici di accesso al servizio[63].

---

[60] Si tratta delle decisioni: Tribunale di Milano del 28/07/2006 in "Diritto dell'Internet", 2007, 62 e segg.; sent. n. 128/08 del Giudice di Pace di Lecce; sent. n. 837/08 del Giudice di Pace di Badolado.

[61] Si tratta del D.lgs. n. 11/2010 ("*Attuazione della direttiva 2007/64/CE, relativa ai servizi di pagamento nel mercato interno, recante modifica delle direttive 97/7/CE, 2002/65/CE, 2005/60/CE, 2006/48/CE, e che abroga la direttiva 97/5/CE*"), nel quale il legislatore ha operato a priori il bilanciamento tra gli interessi spesso opposti di banche e clienti: le prime che vorrebbero scaricare il rischio dell'uso inoculato o illegittimo degli strumenti digitali sui clienti e questi ultimi che vorrebbero essere tutelati in tutti quei casi nei quali non siano stati loro ad usare la carta o a dare l'ordine di pagamento online. Il decreto legislativo ha imposto alle banche, nella loro qualità di prestatori di servizi di pagamento, specifici obblighi di precauzione, primo tra tutti l'obbligo di garantire l'inaccessibilità dei dispositivi di sicurezza di pagamento da parte di soggetti non autorizzati (art. 8 e art. 11); i clienti, dal lato loro, risultano titolari dell'obbligo di custodia con sufficiente accuratezza degli strumenti che servono a disporre i pagamenti, dell'obbligo d'utilizzo corretto e diligente, ed infine di quello di comunicazione tempestiva alla banca di eventuali usi indebiti da parte di terzi (art. 7). Per rafforzare la posizione dei clienti, il decreto in commento ha previsto un deciso *favor* probatorio nei loro confronti, prevedendo che sia onere dell'intermediario, nei casi in cui il cliente neghi di aver dato corso all'operazione, a dover dimostrare la negligenza del cliente (o la sua frode) e che il servizio di pagamento azionato tramite lo strumento affidato al cliente abbia funzionato correttamente. Per quanto attiene specificamente alla posizione del cliente, è necessario valutare caso per caso se i suoi comportamenti possano o meno considerarsi fraudolenti (vale a dire se sussiste la volontà consapevole di ingannare la banca), ovvero negligenti al punto da qualificarsi in "colpa grave", cioè in violazione di quei minimi doveri di diligenza imposti al cliente/utilizzatore.

[62] Decisione n. 46/10 della seduta del Collegio di Milano del 21/01/2010.

[63] In particolare, il Collegio ha osservato che "*la banca la quale offre servizi on-line alla propria clientela ha il dovere di adempiere il proprio obbligo di custodia dei patrimoni dei clienti con la diligenza professionale richiesta dall'art. 1176, c. 2, c.c., predisponendo misure di protezione – tra le quali l'invio di sms di conferma dell'eventuale disattivazione del servizio di SMS-alert e l'invio di sms di avviso dell'esecuzione dell'ordine di bonifico - idonei ad evitare l'accesso fraudolento di terzi ai depositi dei propri clienti, o a neutralizzarne gli effetti. La violazione dell'obbligo di diligenza da parte della banca non esclude, però, la colpa concorrente del titolare del conto on-line, ex art. 1227 c.c., per incauta custodia dei codici di accesso al servizio, nella ipotesi in cui l'operazione fraudolenta sia avvenuta mediante l'uso dei*

In altra decisione[64] l'ABF ha deciso che il cliente andava rimborsato del 75% delle perdite subite in quanto "*il corretto adempimento dell'obbligo di diligenza presuppone l'adozione di tutte le precauzioni e l'istituzione di tutti i presidi di sicurezza adeguati allo scopo e resi accessibili dall'evoluzione scientifica e tecnologica*". Dopo l'ammissione da parte del correntista di aver risposto ad una e-mail rivelatasi un classico caso di "phishing", l'ABF ha ravvisato comunque una colpa nel comportamento della banca perché non ha fornito al cliente dispositivi automatici per la generazione di password, ravvisando in ciò una violazione dell'obbligo di diligenza, mancando l'adeguamento dei presidi "*agli ultimi ritrovati ed alle più recenti acquisizioni della scienza e della tecnologia*".

La strada intrapresa dall'organismo indipendente bancario è sicuramente di pregio, poiché tenta di tradurre nei fatti l'equilibrio fissato a monte dal legislatore, dislocando in maniera equitativa l'effettiva responsabilità del danno in capo ad entrambi i soggetti coinvolti ed evitando di conferire una sorta di immunità ad alcuno: in una situazione come quella del "phishing", l'attacco di regola riesce proprio grazie allo sfruttamento delle debolezze dei soggetti coinvolti, vale a dire l'ingenuità o ignoranza dell'utente e l'obsolescenza o gli errori dei sistemi di sicurezza. Perciò risulta corretto almeno da un punto di vista di giustizia sostanziale distribuire il carico di responsabilità tenendo conto del peso relativo delle mancanze di ciascun soggetto coinvolto.

Nondimeno, la tendenza della giurisprudenza ordinaria più recente è quella di addossare il peso della responsabilità esclusivamente in capo all'intermediario finanziario, sia argomentando a titolo di responsabilità contrattuale sia a titolo di responsabilità aquiliana. Si tratta di un orientamento che rischia di deresponsabilizzare gli utenti, legittimando in loro sentimenti di noncuranza o vero e proprio disinteresse rispetto alle conseguenze di un utilizzo degli strumenti informatici poco avveduto.

Una delle pronunce più interessanti è stata emessa dal Tribunale di Palermo nel

---

codici in suo possesso. Pertanto, ritenendo che la ricorrente, per le ragioni esposte, abbia concorso a cagionare il danno nella misura del 75%, la banca deve essere dichiarata tenuta a rifondere alla ricorrente il 25% della somma di 5.773,00 euro".

[64] Decisione n. 33/10 della seduta del Collegio di Roma del 12/01/2010.

2011[65]: il giudice ha condannato l'azienda Poste Italiane al rimborso integrale delle perdite subite dagli attori, ritenendola, da un lato, responsabile a titolo contrattuale per l'inesatto adempimento delle obbligazioni derivanti dal contratto, con riferimento al prelievo illecito e fraudolento, poiché non aveva predisposto misure di sicurezza idonee ad escludere la possibilità che si verificasse un *bug* nel sistema, né complessivamente adeguate alla tecnologia esistente; dall'altro veniva rilevato un profilo di responsabilità extracontrattuale, sulla base della normativa contenuta nel Codice Privacy (D.lgs. n. 196/2003), che dispone l'obbligo di risarcimento ex art. 2050 c.c. nel caso di danno ad altri per effetto del trattamento di dati personali. Il giudice ha inoltre ritenuto applicabile l'art. 31 del citato decreto, con specifico riferimento al grado di inviolabilità richiesto alle misure di sicurezza[66]: in base a tali previsioni, il canone di diligenza professionale cui la convenuta deve attenersi nell'esercizio della propria attività d'impresa richiede l'adozione di tutte le misure di sicurezza tecnicamente idonee e conosciute a prevenire danni come quelli verificatisi in capo agli attori. Non può essere ritenuta sufficiente la mera non violazione di norme di legge, in considerazione del fatto che la diligenza del professionista deve essere valutata con maggiore rigore rispetto a quella ordinaria.

Tale orientamento giurisprudenziale di deciso *favor* verso i correntisti è stato confermato recentemente da due sentenze del 2014[67]: in entrambi i casi i giudici di merito hanno valutato con estremo rigore la posizione degli intermediari convenuti in giudizio dai propri clienti, vittime di classici casi di "phishing", sostenendo a vario titolo che la violazione degli obblighi inerenti alla predisposizione di dispositivi di sicurezza idonei ad evitare intrusioni nei sistemi comporti il risarcimento integrale del danno patito. In proposito, si cita una sentenza del Tribunale di Milano che dilata ulteriormente i confini della tutela informatica che l'intermediario è tenuto a fornire al proprio cliente: si stabilisce

[65] Trib. di Palermo, sez. II, sent. n. 2904 del 11/06/2011 – Giud. Spiaggia

[66] L'art. 31 D.lgs. 196/2003 stabilisce che "*i dati personali oggetto di trattamento debbano essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta".*

[67] Trib. di Firenze, sez. III civile, sent. del 20/05/2014; Trib. di Milano, sez. VI civile, sent. del 04/12/2014.

infatti che, anche a fronte dell'adozione di misure di protezione in linea con gli standard del settore, costui può essere comunque chiamato a rimborsare la perdita sofferta dal correntista, a norma della disciplina sui servizi di pagamento, nelle ipotesi in cui l'attacco informatico sia posto in essere con modalità particolarmente sofisticate, non riconoscibili e neutralizzabili dal cliente medio. Si tratta di quei casi in cui non può in alcun modo configurarsi la "colpa grave" dell'utente medio, il quale non è in grado di prendere alcuna efficace contromisura contro la tecnica truffaldina utilizzata dal phisher: l'unico soggetto che possiede le risorse tecniche ed economiche per fare in modo che tali elaborati attacchi non si consumino è l'intermediario, che perciò ha l'obbligo di agire sulla base della disciplina dei servizi di pagamento.

È evidente come la strada intrapresa dalla giurisprudenza sia quella di allocare la responsabilità in capo al soggetto che maggiormente dispone delle risorse e delle capacità per bloccare *ab origine* gli attacchi: tuttavia appare criticabile la deresponsabilizzazione che ne deriva in capo all'utente medio, poiché sussiste il rischio concreto che una tutela così ampia lo renda poco attento alle conseguenze delle proprie azioni nella rete[68]. È certo che gli intermediari debbano predisporre sempre le misure di sicurezza migliori e tecnologicamente più avanzate per evitare operazioni fraudolente sui conti dei propri clienti; nondimeno dovrebbero operare in prima linea per rendere gli stessi correntisti dei "guardiani" del sistema, investendo nell'ambito della sensibilizzazione e della divulgazione di conoscenze base sulla cybersecurity. In tal modo sarebbero gli stessi clienti a creare una prima barriera agli attacchi informatici e gli intermediari potrebbero utilizzare come difesa in un eventuale giudizio le prove della loro concreta attività di sensibilizzazione, manifestazione in chiave preventiva della diligenza professionale.

[68] In Germania si registrano posizioni giurisprudenziali più ferree nei confronti dei correntisti: secondo quanto deciso dai giudici della Corte Federale di Giustizia della città di Karlsruhe, Bundesland Baden-Württemberg, i vertici dell'istituto creditizio convenuto in giudizio non possono essere considerati responsabili per una frode telematica perpetrata ai danni di un pensionato del luogo vittima di un caso di phishing. Il tribunale non ha accolto le lamentele del truffato, protagonista di un evidente atto di negligenza; la banca ha evitato di incorrere in responsabilità dimostrando come più volte ha agito con diligenza, informando adeguatamente i propri clienti con campagne di sensibilizzazione contro il Phishing. http://arstechnica.com/business/2012/04/clients-not-banks-liable-for-losses-in-phishing-scams-court-rules/

Capitolo VI: Panorama degli interventi e delle strategie contemporanee per contrastare le frodi informatiche

6.1 Soluzioni in ambito UE ed internazionale

Negli ultimi anni, l'azione dei governi impegnati ad assicurare al cyberspazio un livello adeguato ed effettivo di sicurezza ha trovato riscontro in varie iniziative delle organizzazioni internazionali e sovranazionali incentrate sulla prospettiva d'intervento preventivo. Dagli anni Novanta infatti si è registrata nella maggior parte delle legislazioni occidentali una tendenza comune, consistita nel progressivo allontanamento dall'idea di diritto penale "panacea" per tutte le problematiche sociali ed economiche. Si sta progressivamente riscoperto il principio di *extrema ratio* che deve sempre orientare il legislatore penale, affiancando quindi tale tipo di intervento a quello degli altri rami del diritto: in altri termini, il fallimento dell'ipertrofia dei sistemi penali contemporanei sta facendo riscoprire l'importanza degli interventi di tipo preventivo e non repressivo, l'attuazione dei quali è demandata a rami del diritto diversi da quello penale.

I motivi di tale cambiamento di prospettiva sono molteplici e molti autorevoli giuristi non hanno mancato di rilevarli: alcune tipologie di reati, fra le quali sicuramente i computer crimes, godono di una diffusa tolleranza a livello sociale quando vengono posti in essere a livello "domestico", poiché sono generalmente percepiti come poco o nulla offensivi. Ciò determina una scarsità di denunce[1], accompagnata quindi dalla difficoltà di accertamento delle reali perdite connesse al fenomeno. È pur vero che anche nell'eventualità in cui venga presentata querela, le indagini risultano difficoltose: nella maggior parte dei casi, l'hacker ha già fatto perdere le proprie tracce, grazie all'anonimato di cui di regola gode e alla velocità delle operazioni nella rete, luogo in cui le

[1] Secondo Don Parker, il rapporto fra crimini denunciati e crimini realmente commessi si aggira attorno all'uno per cento. Anche l'entità delle perdite non può essere accertata in modo univoco. La "cifra oscura" non sarà mai realmente individuabile ma si può sostenere con certezza che i reati informatici denunciati sono la minima parte rispetto al numero totale di cybercrime commessi; "*The cost of crime against business*", US Departement of Commerce, Washington; C. Sarzana di S. Ippolito, *op.cit*.

distanze spazio-temporali sono praticamente annullate. Spesso inoltre le forze dell'ordine non sono dotate dell'apparecchiatura necessaria per indagare con successo questi illeciti, sussistendo un *gap* tecnologico fra gli strumenti in uso alle stesse e i dispositivi di cui si servono i criminali informatici; a ciò si aggiunga che molti atti d'indagine risultano particolarmente complessi ovvero comportano costi elevati, sia dal punto di vista economico sia dal punto di vista delle risorse umane impiegate e dei tempi richiesti (per es. una rogatoria internazionale). Accade quindi spesso che nei casi di frode informatica di poche centinaia di euro o non venga affatto presentata la querela, poiché la persona offesa è in qualche modo già rassegnata all'impossibilità di riavere il proprio denaro, ovvero dopo la denuncia l'iter investigativo si areni a causa delle difficoltà di coordinamento internazionale e della mancanza di strumenti d'indagine adeguati. Quando poi le frodi informatiche sono poste in essere da hacker tecnologicamente esperti e con target più redditizi (istituti di credito, infrastrutture sensibili), le difficoltà di accertamento non diminuiscono, data la riluttanza delle imprese a denunciare gli attacchi informatici di cui sono vittime, temendo di mostrarsi vulnerabili agli occhi dei clienti relativamente alla sicurezza dei propri sistemi.

Grande problema legato a doppio filo alle frodi informatiche consiste quindi negli altissimi costi sociali direttamente derivanti dalle stesse, sia in termini di profitto per l'agente e conseguente danno per la persona offesa, sia in termini di costi economici e temporali delle indagini, vista la necessità di competenze specifiche, strumentazione tecnologicamente evoluta e richiesta di supporto ed interazione a livello internazionale.

Come accennato, la difficoltà di individuazione dei responsabili deriva anche dall'anonimato permesso da un lato dalla stessa conformazione della rete internet, poiché non si può mai sapere con certezza chi si cela dietro un nickname o un codice d'accesso utilizzato in un sistema informatico, dall'altro dall'assenza di confini della spazio cibernetico, che così diventa uno spazio globalizzato, distesa immensa e infinita contrapposta alla parcellizzazione delle giurisdizioni statali. I criminali più esperti possono sfruttare a proprio vantaggio le difficoltà di coordinamento che sempre sussistono quando le indagini

interessano più territori statali.

Una lunga serie di motivazioni ha quindi portato gli interventi sovranazionali degli ultimi anni a muoversi in chiave preventiva, essenzialmente seguendo due direttrici: da un lato implementando la sicurezza del cyberspazio e in generale delle transazioni, attraverso obiettivi strategici comuni, direttive per le legislazioni nazionali, regole condivise per il coordinamento delle indagini internazionali, ed organismi sovranazionali con il compito di controllare l'effettività del coordinamento e la formazione in ambito informatico, in modo tale che internet possa diventare una piattaforma funzionale allo sviluppo economico e sociale; dall'altro tutelando l'identità individuale come complesso di dati sensibili inerenti ad una persona, la quale deve avere pieno diritto di decidere se e come utilizzarli e divulgarli, sia nel cyberspace sia nel mondo reale. La prevenzione di fatto risulta essenziale poiché permette di evitare di appesantire notevolmente il carico di lavoro delle procure e degli organi di polizia postale, i quali potrebbero così occuparsi con più efficienza solo di quei casi che siano davvero complessi, nei quali la normale accortezza e diligenza dei cybernauti non risulta sufficiente ad evitare il danno.

Il primo strumento che realmente può avere capacità preventiva in settori ad alto tasso di specificità delle conoscenze richieste per l'azione sia dei criminali sia di corpi d'intelligence consiste nella diffusione, implementazione e condivisione di informazioni: i criminali informatici spesso riescono ad avvantaggiarsi di *gap* nelle informazioni su di loro e su come agiscono, causati dalla difficoltà di trasmissione e condivisione delle conoscenze, dalla scarsa *expertise* delle forze di polizia e anche, purtroppo, dalla diffusa reticenza – sia nel settore pubblico sia in quello privato – nel condividere informazioni relative a cybercrimes subiti. Solo riequilibrando la situazione informativa fra i criminali informatici e gli apparati pubblico-privati di contrasto è possibile porre in essere i comportamenti più consoni ai fini preventivi: al riguardo la sensibilità più recente sta cambiando, infatti si stanno affermando sia nel settore pubblico sia nel settore privato vari sistemi per condividere informazioni, o basati semplicemente sullo sviluppo di grandi database a partecipazione volontaria ovvero legati alla creazione di organismi sovranazionali che fungano da

collettore di informazioni e di sviluppo di studi d'analisi.

Gli approdi degli studi criminologici degli anni Novanta in tema di prevenzione situazionale[2] e della particolare branca del diritto che analizza le componenti dell'ordinamento giuridico attraverso concetti e modelli economici[3] hanno permesso di definire meglio le modalità concrete in cui dovrebbe realizzarsi l'azione governativa più efficace ed efficiente. Le misure preventive dovrebbero tendere a rendere il crimine, nella specie l'illecito informatico, meno attrattivo per chi lo commette: ad oggi, ci sono troppi pochi rischi potenzialmente derivanti dalla commissione di una frode informatica, e ciò la rende "invitante". Fulcro degli studi giuseconomici da un lato e della prevenzione situazionale dall'altro è l'idea che il crimine possa essere in una certa misura attrattivo e che, a parità di guadagni, possa persino diventarlo più di altre attività lecite: perciò per essere efficace ed efficiente, il sistema di prevenzione deve rendere l'atto criminale più difficile, più rischioso e meno proficuo rispetto alle alternative lecite, per un'ampia gamma di aggressori, al costo minore; volgendo il ragionamento in termini economici, ciò significa che l'ordinamento deve evitare che l'utilità attesa derivante dal compimento dell'atto illecito sia maggiore rispetto alle alternative lecite, al netto dei costi[4]. Oltre alle valutazioni materiali,

[2] Uno dei più importanti sostenitori di questo approccio criminologico fu R. V. Clarke, professore di Criminal Justice nella Rutgers University (New Jersey) e attivo collaboratore per molti anni con il Ministero dell'Interno inglese. Fra i suoi scritti si ricorda "*Situational Crime Prevention: Successful Case Studies*", 1997, 2nd Edition, Albany, NY: Harrow & Heston.

[3] L'analisi economica del diritto è nata a cavallo degli anni Cinquanta e Sessanta come ausilio soprattutto negli specifici ambiti del diritto civile e commerciale, dove l'applicazione di concetti e modelli matematici al diritto viene considerato un utile strumento in grado di fornire soluzioni efficienti. Al contrario, nell'ambito del diritto penale e del sistema della giustizia penale ha avuto scarsa influenza e fatica ancor oggi a ritagliarsi una legittimazione accanto alle tradizionali teorie della redistribuzione e della prevenzione generale negativa. F. Pesce, "*Alle radici di un difficile binomio: analisi economica e diritto penale*", in Indice Penale – nuova serie, anno XIV, n. 1, Gennaio-Giugno 2011, Cedam.

[4] L'idea che il criminale sia un soggetto massimizzatore di utilità e che sia necessario prevenire le sue azioni non sono un contributo originale degli economisti del secondo dopoguerra. La paternità di queste acquisizioni è in realtà da attribuire al pensiero filosofico di Montesquieu, Beccaria e Bentham. Montesquieu individuò la funzione della legge penale come distributrice di incentivi per gli individui. Beccaria ipotizzò un approccio sistematico al diritto penale ideando quella che oggi viene intesa come una prospettiva di analisi economica del diritto: nelle prime pagine dei "*Delitti e delle pene*" Beccaria collega la legge penale alla necessità di prevenire i comportamenti antisociali di coloro che seguono razionalmente il proprio tornaconto personale. Il problema di individuare un criterio di misurazione degli incentivi era poi ben presente a Bentham, il quale lo formula facendo ricorso alla terminologia delle scienze esatte che e` alla base del pensiero illuminista e dell'economia politica moderna: "...*il profitto del criminale e` la forza che lo spinge a delinquere: il costo della punizione e` la forza che lo trattiene. Se la prima*

talvolta è utile tenere conto anche dei "costi morali", dunque è necessario mettere in campo azioni che rendano più arduo per gli aggressori giustificare le proprie azioni[5]. Sia l'analisi economica del diritto sia lo studio criminologico si soffermano perciò sulle circostanze che inducono ad un tipo specifico di crimine, siano esse di tipo normativo-ordinamentale ovvero socio-ambientale: da esse è possibile elaborare opportune strategie di politica criminale e dedurre quali cambiamenti situazionali siano in grado di ridurre le possibilità che un determinato illecito venga posto in essere. In particolare, l'analisi economica del diritto penale tenta di porsi come strumento per giustificare l'esistenza delle maggiori teorie del reato e della pena, razionalizzarne gli obiettivi e le potenzialità, al fine di migliorarne le prestazioni. La maggiore attenzione è dedicata alla teoria della funzione generalpreventiva negativa della pena, in particolare al mondo del c.d. *enforcement* delle norme penali, vale a dire l'insieme di strumenti per l'applicazione, il controllo ed il rispetto delle stesse: si

---

di queste forze prevale, il crimine viene commesso; se prevale la seconda, il crimine non sarà commesso". Circa duecento anni dopo, del resto, nel suo contributo fondamentale all'analisi economica dei delitti e delle pene, G. Becker nell'opera fondamentale "*Crime and Punishment: Economy Approach* (1968)" dichiara esplicitamente di voler riprendere in chiave moderna il pensiero classico. Il comportamento criminale, secondo Becker, può essere spiegato all'interno di una generale teoria economica per la quale il numero dei reati commessi da un individuo dipende dalla valutazione fatta dal potenziale reo sulla probabilità di essere condannato, dalla presunta severità della sanzione, e da altre variabili come il reddito disponibile per attività legali o illegali, variabili ambientali, e variabili legate alla volontà di commettere un atto illegale. La formula base del pensiero di Becker è O=O(p, f, u,). Per un approfondimento: F. Pesce, "*Alle radici di un difficile binomio: analisi economica e diritto penale*", in Indice Penale – nuova serie, anno XIV, n. 1, Gennaio-Giugno 2011, Cedam.

[5] E. Eide tentò di innestare le norme all'interno dello schema tradizionale della scelta razionale elaborato da Becker. A tal fine egli ipotizzò che i desideri dell'individuo riguardino non solo gli esiti delle azioni, dai quali dipende il grado di soddisfazione dei propri bisogni, ma anche l'adesione a determinate norme che regolano la vita degli individui e che sono particolarmente sentite e rispettate dagli stessi perché coinvolgono la loro sfera morale L'ambito delle preferenze individuali, pertanto, si compone di due elementi: i bisogni (per gli esiti) e le norme (attitudini morali). Per appagare i propri bisogni l'individuo guarda alle conseguenze delle possibili opzioni, ma, allo stesso tempo, l'adesione alle norme richiede di prediligere o scartare determinate linee di condotta. L'individuo deve perciò bilanciare azioni e risultati, soddisfazione dei bisogni e adesione alle norme. Una norma infatti può rivestire una grande importanza a causa del disagio, o senso di colpa, che prova l'individuo nel momento in cui la infrange, ma se un'azione trasgressiva rispetto alla norma assicura un esito altamente desiderato, l'individuo potrebbe benissimo decidere di agire in contrasto con essa. Le norme possono restringere la gamma di azioni dell'individuo senza tuttavia essere vincolanti, oppure possono assumere un peso tale da ridurre il repertorio di azioni ammissibili a poche o, al limite, ad una sola: quella prescritta dalla norma. E. Eide, "*Economics of Criminal Behavior*", *The Economic Journal*, 1981, p. 353 in F. Pesce, "*Alle radici di un difficile binomio: analisi economica e diritto penale*", in Indice Penale – nuova serie, anno XIV, n. 1, Gennaio-Giugno 2011, Cedam.

tratta in sostanza di capire quali siano gli strumenti e i metodi più efficaci al fine di individuare chi delinque, imporre le conseguenti sanzioni e fare in modo che i cittadini, da un lato, si astengano dal commettere reati, dall'altro, siano incentivati a conformare il proprio comportamento alle regole. Tanto maggiore è l'efficienza dell'apparato di enforcement, tanto più forte sarà la sua azione generalpreventiva, direttamente derivante dalla certezza delle sanzioni nonché dalla disincentivazione di potenziali condotte illecite. Ogni ordinamento che aspiri a compiere scelte efficienti – aumentando così il benessere totale – deve aver ben presente che l'efficacia di una normativa deriva direttamente dall'efficacia del suo apparato di enforcement: deve perciò rendere quanto più concreta ed effettiva possibile (sia in termini di probabilità dell'accertamento che di forza dissuasiva della sanzione) l'implementazione di un dato precetto normativo. L'analisi economica del diritto analizza i vari strumenti di enforcement anche al fine di individuare le sanzioni (sia nell'an che nel quantum) ottimali. Enforcement e politica sanzionatoria sono, quindi, due realtà strettamente correlate; un enforcement efficiente, infatti, può non solo diminuire gli illeciti, ma può anche determinare una minore dannosità in termini di costo collettivo, delle violazioni che comunque vengono commesse. Ogni teoria economica deve tener in considerazione i costi sottesi alle singole scelte: perciò anche la scelta di applicare in una certa misura e con certe modalità (grado di severità e certezza della pena) la legge penale comporta un costo, in termini di perdita di benessere sociale: è un concetto spesso trascurato ma di rilevanza fondamentale in un sistema giuridico che miri davvero a raggiungere i propri obiettivi. I giureconomisti declinano di regola tale costo nella somma di tre elementi: la perdita del reddito reale causata dai crimini, il costo del sistema giudiziario, il costo sociale delle punizioni. L'analisi economica del diritto tenta proprio di fornire delle soluzioni per individuare l'equilibrio più efficiente fra l'insieme dei costi derivanti direttamente e indirettamente dal crimine e il benessere sociale collettivo, utilizzando le regole e i modelli propri della microeconomia, la quale sfrutta molte teorie dei comportamenti (es. la teoria del comportamento razionale dell'*homo oeconomicus*) e strumenti analitici in grado

di fornire utili risultati per valutare l'efficienza allocativa delle norme[6].

Dal canto suo, la prevenzione situazionale si concentra sullo studio delle motivazioni e delle precondizioni che rendono invitante un determinato illecito, piuttosto che sugli autori degli atti criminali: non cerca di individuare il modo per fermare il criminale, essendo la sua scelta quasi la "naturale" conseguenza di un insieme di fattori propulsivi, di tipo normativo, psicologico, ambientale e sociale. Seguendo i suggerimenti volti ad evitare la creazione di opportunità criminali[7], la riduzione della criminalità dovrebbe essere un beneficio collaterale derivante dalla tecniche di prevenzione. L'attenzione di questa teoria non si concentra sul sistema di giustizia penale ma su un insieme di organizzazioni pubbliche e private e di agenzie (scuole, ospedali, sistemi di trasporto, negozi e centri commerciali, piccola imprenditoria e compagnie telefoniche, parchi locali e luoghi di divertimento, bar e parcheggi) i cui prodotti, servizi ed operazioni creano opportunità per una vasta gamma di reati. Sono quindi questi stessi soggetti che dovrebbero porre in essere le misure tecniche di prevenzione più corrette per arginare le fattispecie delittuose.

In ambito europeo e internazionale sono state organizzate varie iniziative per implementare la cooperazione e la diffusione di informazioni fra gli Stati contraenti: molto è stato fatto ma molto si deve ancora fare, soprattutto nei riguardi di quelle frodi informatiche che non coinvolgano direttamente le istituzioni europee e non causino danni economici rilevanti (si tratta di quelle numericamente più alte).

6.1.1. OLAF: Ufficio Europeo Antifrode

Per quanto attiene strettamente alla tutela degli interessi finanziari dell'Unione Europea, è stato istituito nel 1999 l'Ufficio europeo di lotta antifrode

[6] F. Pesce, "*Alle radici di un difficile binomio: analisi economica e diritto penale*", in Indice Penale – nuova serie, anno XIV, n. 1, Gennaio-Giugno 2011, Cedam.

[7] Alcuni di questi possono sembrare scontati ma si è potuto verificare come siano condizioni assolutamente rilevanti per la proliferazione di opportunità criminali: ad esempio, l'illuminazione delle strade cittadine assume un ruolo centrale rispetto all'aumento o alla diminuzione di illeciti come il furto o la rapina. Clarke, R.V., "*Situational Crime Prevention: Successful Case Studies*", 1997, 2nd Edition, Albany, NY: Harrow & Heston, pp. 2-43.

(OLAF), sostituendo l'Unità di coordinamento della lotta antifrodi (UCLAF) creata dalla Commissione dieci anni prima, la quale aveva avuto un ambito operativo più limitato. Si tratta di un organismo direttamente dipendente dalla Commissione europea – nella persona del Vicepresidente – che si occupa precipuamente della lotta contro le frodi che possano comportare un depauperamento delle finanze europee. Tale iniziativa si inserisce nel quadro della "cooperazione di Polizia e Giudiziaria in materia penale" e contemporaneamente testimonia la crescente consapevolezza delle autorità dei singoli Stati membri dell'importanza di una azione coordinata in questo settore: l'aggressione alle risorse economiche europee colpisce in via indiretta gli stessi Stati membri dell'Unione e i loro contribuenti, determinando perdite negli investimenti e in generale nelle potenzialità di crescita sociale ed economica collettiva.

All'OLAF sono attribuite ampie funzioni nell'ambito specifico della lotta alle frodi alle risorse finanziarie europee: svolge una funzione investigativa, attribuitagli dalla Commissione nell'ambito della normativa comunitaria e degli Accordi con i Paesi terzi, al fine di dare una risposta incisiva contro le frodi, la corruzione e qualsiasi altra attività illegale che danneggi gli interessi finanziari dell'Unione Europea. Godendo di piena indipendenza operativa e amministrativo-contabile, l'Ufficio ha il compito di svolgere sia indagini interne, in qualsiasi istituzione e organo europei finanziati dal bilancio dell'UE, sia indagini esterne, a livello nazionale, quando vi è il sospetto di frode alle risorse finanziarie europee. A tal fine, l'OLAF ha facoltà di effettuare controlli in loco ed ispezioni nelle sedi degli operatori economici, in stretta collaborazione con le autorità competenti degli Stati membri o dei Paesi terzi. L'OLAF è altresì punto di riferimento per soggetti pubblici e privati per l'invio di segnalazioni su frodi e irregolarità, che permettano poi di svolgere indagini più approfondite. Nella maggior parte dei casi, le informazioni sono il risultato di controlli effettuati da chi è responsabile della gestione dei fondi dell'UE nelle istituzioni europee o negli Stati membri.

I risultati delle indagini dell'OLAF hanno un impatto sostanziale a livello interno e conferiscono effettività alla sua azione: possono infatti essere ammessi come prove nei procedimenti penali degli Stati membri. Per la prima volta un organo

sovranazionale ha la possibilità di raccogliere elementi di prova ai quali l'ordinamento comunitario assicura poi una efficacia diretta nei singoli Stati membri[8].

Lavorando nell'alveo degli Uffici della Commissione, l'OLAF è chiamato ad assistere le istituzioni europee, in particolare la stessa Commissione, nell'elaborazione e attuazione della legislazione, di metodi di prevenzione e di strategie comuni antifrode. Si occupa anche di attività di formazione, studio e coordinamento dell'azione dei singoli Stati membri per contrastare al proprio interno le frodi a danno del bilancio europeo: in particolare, si pone come ente di collegamento costante sia fra gli Stati membri (legislatore, autorità giudiziarie e autorità di polizia) e la Commissione sia tra le Autorità nazionali competenti, rendendo la collaborazione più agevole, stretta e regolare.

Una delle più importanti attività dell'OLAF a sostegno della repressione delle frodi ai danni dell'Unione Europea consiste nei programmi Hercule (I-II-III), con i quali dal 2004 vengono stanziate cospicue risorse per rafforzare e rendere più efficaci gli interventi statali in questo settore, al fine ultimo di creare un'economia europea più competitiva e capace di garantire la protezione del denaro dei contribuenti nel mondo virtuale. Il primo programma Hercule (2004-2006) ha avuto una dotazione finanziaria di circa 12 milioni di euro e aveva una serie di obiettivi importanti, fra cui il sostegno ad attività di studio, formazione accademica e sensibilizzazione, il coordinamento delle attività che riguardano la tutela degli interessi finanziari dell'Unione, lo sviluppo e la messa a disposizione di strumenti informatici specifici per rendere più efficace l'attività degli organi di polizia dei singoli Stati, infine la promozione e il rafforzamento dello scambio di dati. Gli organismi che hanno potuto beneficiare di una sovvenzione nel periodo 2004-2006 sono state le amministrazioni nazionali e regionali, gli istituti di ricerca e d'insegnamento e le organizzazioni senza fini di lucro. Durante la programmazione 2007-2013 il programma Hercule II ha permesso di realizzare 70 progetti di assistenza tecnica e attività di formazione antifrode per oltre 5.300

[8] Oltre alla tutela degli interessi finanziari, l'Ufficio è responsabile di tutte le attività d'indagine sulle irregolarità più gravi connesse all'esercizio di un'attività professionale da parte dei membri e del personale interno alle istituzioni e agli organi dell'UE che possono condurre a procedure disciplinari o penali.

addetti. Per il programma Hercule III 2014-2020 sono stati stanziati 13,7 milioni di euro, che dovrebbero finanziare azioni contro la frode, la corruzione e qualsiasi altra attività illecita che possa ledere gli interessi finanziari dell'Ue. Nello specifico, vengono stanziati finanziamenti per progetti volti al supporto tecnico-operativo specializzato alle autorità degli Stati membri preposte all'applicazione della legge nella lotta contro le attività transfrontaliere illegali; vengono inoltre finanziati l'organizzazione di una formazione specializzata degli operatori del settore e seminari di formazione sull'analisi dei rischi e conferenze (3,4 milioni di euro)[9].

6.1.2. Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA)

L'Agenzia Europea per la sicurezza delle reti e dell'informazione è stata istituita nel 2004 con sede sull'isola di Creta al precipuo fine di contribuire allo sviluppo della cultura della sicurezza informatica relativamente alle informazioni

[9] Il programma dispone un sostegno finanziario per le seguenti azioni:
- assistenza tecnica specializzata alle autorità nazionali che consiste nel: fornire conoscenze specifiche, nonché materiale specialistico e tecnicamente avanzato e strumenti informatici efficaci che agevolino la cooperazione transnazionale e la cooperazione con la Commissione; offrire il sostegno necessario e agevolare le indagini, in particolare tramite l'istituzione di gruppi d'indagine congiunti e di operazioni transnazionali; sostenere la capacità degli Stati membri di immagazzinare e distruggere le sigarette sequestrate, nonché i servizi di analisi indipendenti per l'analisi delle sigarette sequestrate; promuovere gli scambi di personale nell'ambito di progetti specifici, soprattutto nel campo della lotta al contrabbando e alla contraffazione di sigarette; fornire un supporto tecnico e operativo alle autorità degli Stati membri preposte all'applicazione della legge nella lotta contro le attività transfrontaliere illegali e la frode lesive degli interessi finanziari dell'Unione, ivi compreso in particolare il sostegno alle autorità doganali; rafforzare la capacità informatica in tutti gli Stati membri e i paesi terzi, sviluppando e mettendo a disposizione banche dati e strumenti informatici specifici che agevolino l'accesso ai dati e la loro analisi; intensificare lo scambio di dati, sviluppando e mettendo a disposizione gli strumenti informatici per le indagini e sorvegliando le attività di intelligence.
- organizzazione di formazione specializzata e seminari di formazione sull'analisi dei rischi e conferenze al fine di: promuovere una migliore comprensione dei meccanismi dell'Unione e nazionali; realizzare scambi di esperienze tra le autorità competenti degli Stati membri e i paesi terzi, nonché fra i rappresentanti di organizzazioni internazionali, inclusi i servizi di contrasto specializzati; coordinare le attività degli Stati membri, dei paesi terzi e di organizzazioni pubbliche internazionali; divulgare le conoscenze, in particolare sulle migliori modalità di individuazione del rischio a scopo investigativo; sviluppare attività di ricerca emblematiche, compresi gli studi; migliorare la cooperazione fra gli esperti sul campo e i teorici; sensibilizzare ulteriormente i giudici, i magistrati e altri professionisti del settore legale alla tutela degli interessi finanziari dell'Unione.
- qualsivoglia altra azione prevista dai programmi di lavoro annuali necessaria al conseguimento degli obiettivi generali e specifici del programma.
Per approfondimenti: http://ec.europa.eu/anti_fraud/policy/hercule-iii/index_en.htm

condivisibili in rete ed in generale alla sensibilizzazione rispetto alla diffusione di dati nel cyberspace. Si tratta di un'Agenzia europea con compiti prettamente tecnici, che affianca l'operato della Commissione e dei singoli Stati membri a beneficio dei cittadini, dei consumatori, delle imprese e del settore pubblico europei, favorendo lo sviluppo del mercato interno.

L'obiettivo di ENISA è, da un lato, potenziare la capacità di reazione e gestione dei problemi relativi alla sicurezza delle reti e della diffusione di informazioni, dall'altro, lo sviluppo di strategie efficaci di prevenzione: suoi naturali interlocutori sono la stessa Unione Europea, nell'organo Commissione, i Paesi membri ed il settore privato (imprese, istituti di credito, assicurazioni).

Il suo supporto tecnico si sostanzia nell'attività di assistenza e consulenza alla Commissione e alle autorità nazionali attraverso studi, analisi strategiche, valutazioni tecniche e gestione dei rischi (per es. *National-level Risk Assessment* del 2013), realizzate da un gruppo di esperti selezionati fra i più competenti studiosi della materia informatica degli Stati membri; può altresì essere chiamata ad assistere la Commissione e il Parlamento europeo nei lavori tecnici preparatori all'aggiornamento e allo sviluppo della normativa comunitaria per i prodotti e servizi in materia di sicurezza delle reti.

Si occupa anche di sensibilizzazione e formazione, cercando di agevolare ed incoraggiare la cooperazione tra gli operatori del settore pubblico e privato attraverso consulenze, networks, nonché lo scambio di *best practices*, fra le quali rilevano i metodi di allarme degli utenti; con specifico riguardo agli utilizzatori, ENISA si impegna a mettere celermente a loro disposizione informazioni obiettive e complete su tutti i temi legati alla sicurezza delle reti e dell'informazione, permettendo così di migliorare costantemente il livello di sicurezza reale e percepita nelle reti dei Paesi dell'UE.

Infine presenta le proprie conclusioni e i propri orientamenti agli interlocutori internazionali e fornisce consigli agli utenti finali, come la lista del 2009 dei 13 consigli per evitare le frodi con le carte magnetiche[10].

[10] Si tratta di 13 regole di buonsenso facilmente condivisibili, ma l'impatto delle stesse è stato notevole sulla rete poiché hanno trovato rapida diffusione: 1) Non utilizzate apparecchi bancomat che presentino indicazioni o avvertimenti palesemente eccessivi (spesso i truffatori scrivono un gran numero di tali avvisi nei pressi della macchinetta per indurre la vittima a

Negli ultimi anni, molte risorse di ENISA hanno finanziato la ricerca e lo studio nell'ambito delle frodi nei pagamenti online. In questo settore, gli istituti di credito sono spesso la vera vittima ultima delle frodi ai correntisti, essendo tenuti al risarcimento del danno nel caso di cyber-attacco: conseguentemente le misure di sicurezza delle banche, in relazione a conti e pagamenti online, dovrebbero tenere conto del fatto che i PC dei clienti sono o possono essere infetti. Solo sulla base di questa presunzione gli standard di sicurezza delle banche possono considerarsi adeguati e permettono all'istituto di non essere chiamato in corresponsabilità.

Questa presa di posizione segue l'analisi di un recente caso di frode telematica che ha avuto luogo in Olanda, denominata "*High rollers*"[11]. Enisa ha inoltre

---

fidarsi). Cautela se compaiono istruzioni insolite su come utilizzare il bancomat. 2) Utilizzate gli sportelli bancomat all'interno delle banche, ove ciò sia possibile (i bancomat in strada sono più facilmente manomissibili). 3) Non utilizzate sportelli bancomat che non siano adeguatamente fissati al muro (evitare i bancomat "semovibili" e optate per quelli al riparo che costituiscono parte integrante di un edificio). 4) Massima attenzione a ciò che vi circonda, utilizzate sempre sportelli bancomat ben visibili e ben illuminati. Siate oltremodo prudenti con gli sportelli automatici collocati in aree buie o in luoghi che vi sembrano poco controllati e frequentati. 5) Controllate che chi è in coda dietro di voi si tenga ad a una distanza ragionevole. Prudenza e diffidenza verso sconosciuti che si prestino ad offrire aiuto in caso di eventuale blocco o di altre difficoltà nell'uso della carta. 6) Proteggete il vostro Pin coprendo con la mano la tastiera. Ciò al fine di evitare che una telecamera nascosta o una persona nelle vicinanze possa intercettare il vostro codice. Non rivelare mai a nessuno il vostro Pin. 7) Osservare attentamente il frontalino dello sportello bancomat. Se esso appare diverso da altri della stessa zona (per esempio ha uno specchio in più sul davanti), o presenta dei residui di colla (lasciati forse da un apparecchio incollato sopra), o anche istruzioni e indicazioni in sovrappiù, servitevi presso un altro bancomat e informate immediatamente gli impiegati della banca di tali perplessità. 8) Osservate attentamente la fessura nella quale infilare la vostra carta. Se la fessura della carta vi sembra anche solo vagamente strana o presenta delle irregolarità nella sua conformazione, prima di inserire la carta provate a spingere la fessura con le mani. Se qualcosa è stato attaccato sopra il vero lettore, si muoverà o potrà addirittura cadere. I dispositivi concepiti per trattenere carte e contanti devono essere incollati o fissati con il nastro adesivo al lettore di carte o al dispositivo che eroga le banconote. Se l'apparecchio bancomat dovesse presentare qualcosa attaccato alla fessura delle carte o anche alla tastiera, non fatene uso. Annullate la transazione in corso e allontanatevi. Non cercate di rimuovere eventuali dispositivi sospetti. 9) Osservate attentamente la tastiera sulla quale digitare il Pin. Anche se siete abituali frequentatori di uno sportello bancomat, prestate grande attenzione a qualsiasi differenza o a caratteristiche insolite presenti sulla tastiera sulla quale digitate il vostro Pin. Se una falsa tastiera è stata incollata sopra quella vera, vi apparirà sicuramente "fissata male" allorché cercherete di spostarla avanti e indietro. 10) Controllate che non vi siano troppe telecamere. Se vi siano telecamere in più oltre a quelle ovvie, prestare massima attenzione perché una di quelle potrebbe essere di troppo. 11) Denunciare immediatamente le carte trattenute e, ove possibile non allontanatevi dallo sportello mentre telefonate alla banca, quindi avvisate immediatamente le forze dell'ordine. 12) Prestare attenzione se lo sportello automatico non eroga contanti o non addebita spese di utilizzo. In tal caso potrebbe trattarsi di un bancomat falso. 13) Controllate di frequente gli estratti conto. Le operazioni sospette devono essere contestate entro sessanta giorni dall'esborso tramite raccomandata con ricevuta di ritorno.

[11] Vedi il rapporto "*Dissecting Operation High Roller*" diffuso nel 2012 da due imprese

raccomandato l'adozione di devices e strumenti ad hoc (inclusi gli smartphones) per assicurare la sicurezza dei conti online, e maggiore cooperazione transfrontaliera.

Le banche quindi dovranno dimostrare di aver predisposto strumenti di sicurezza sempre più sofisticati al fine di evitare corresponsabilità nel caso di frodi telematiche: le misure di protezione dovranno essere talmente efficaci da ridurre al minimo anche il rischio potenziale di attacco informatico.

6.1.3. *European Cybercrime Centre* (EC3)

Secondo la Commissione europea ogni giorno dai 250mila ai 600mila account Facebook sono chiusi a causa di tentativi di accesso abusivo. Virus di ogni tipo e "cavalli di Troia" hanno infettato oltre 6 milioni e 700mila computer solo nel 2009. Anche la diffusione di carte di credito clonate ha raggiunto livelli allarmanti: d'altronde per comprarne una è sufficiente navigare un po' e, passando da sito a sito, se ne trovano facilmente a tre cifre con pochi euro di spesa.

Per combattere efficacemente i sempre più diffusi reati informatici, l'11 gennaio

---

specializzate in sicurezza informatica, Guardian Analytics e McAfee. A differenza degli attacchi informatici standard, di solito caratterizzati dalla necessità di intervento da parte dell'uomo, nell'operazione *High Roller* sono stati scoperti almeno una dozzina di gruppi che utilizzavano prettamente componenti automatizzate, fra le quali server posizionati in vari Stati in USA, Europa e Asia, malware dal funzionamento ormai consolidato e un database automatizzato di account di persone i cui conti correnti avrebbero permesso l'effettivo trasferimento di denaro. Aggirando la necessità di un'autenticazione fisica, ogni attacco risultava rapido e difficilmente ricostruibile: l'operazione combinava un livello molto elevato nella conoscenza dei sistemi di transazione bancaria acquisito grazie allo studio degli stessi "dall'interno" e un malware che si installava fraudolentemente nel PC della vittima, attivandosi in maniera automatizzata all'avvio di ogni nuova sessione di home banking. Veniva così prelevato denaro dal conto online del correntista senza che lui potesse accorgersene e il malware lo faceva pervenire sui conti correnti online dei soggetti elencati nel database, i quali si prestavano per il riciclo di denaro. L'organizzazione criminale aveva attivato oltre 60 server in tutto il mondo, presso i quali aveva aperto falsi account utilizzati poi come destinazione dei furti di denaro dai conti correnti online. Gli account erano collegati a carte di debito prepagate e anonime da cui i soldi venivano prelevati rapidamente. A essere presi di mira sono stati soprattutto clienti privati con elevate somme di denaro sui conti correnti o aziende e professionisti.

I criminali hanno effettuato migliaia di trasferimenti per un valore di almeno 60 milioni di euro dai conti di oltre 60 istituzioni finanziarie in Europa, America Latina e Stati Uniti: alcuni trasferimenti sono arrivati a cifre piuttosto cospicue, anche 100.000 euro. Se tutti i tentativi di frode avessero avuto successo – come l'esempio olandese – il tentativo di frode totale potrebbe essere valutato per due milioni di euro.

2013 (solo sei mesi dopo che la decisione fu presa)[12], su richiesta del Consiglio, è stato inaugurato il nuovo Centro europeo per la lotta alla criminalità informatica (EC3) all'Aja presso l'Ufficio europeo di polizia (Europol), con lo scopo primario di contribuire a proteggere i cittadini e le imprese europei dalla criminalità informatica, in particolar modo a garanzia dei minori ovvero di soggetti comunque deboli e inesperti. Ogni attività illecita realizzata attraverso internet, incluse le frodi con carte di credito e su conti bancari e senza dimenticare la protezione dei profili dei social network e dei dati sensibili viene monitorata dal Centro, il quale segnala agli Stati membri le minacce e fornisce avanzati strumenti di difesa, attraverso il sostegno operativo alle indagini. Cecilia Malmström, all'epoca Commissaria UE per gli Affari interni, partecipando all'inaugurazione ufficiale del Centro, ha affermato: "*Il Centro per la lotta alla criminalità informatica darà un forte impulso alla capacità dell'UE di combattere la criminalità informatica e proteggere una rete internet libera, aperta e sicura. I criminali informatici sono intelligenti e veloci nell'utilizzare le nuove tecnologie per scopi criminali; il Centro EC3 ci aiuterà a diventare ancora più intelligenti e veloci al fine di contribuire a prevenire e combattere i reati informatici*".

Nella lotta alla criminalità informatica, globalizzata e caratterizzata da una grande abilità dei criminali a rimanere anonimi e "inesistenti" agli occhi dell'utente, è necessaria una risposta flessibile e adeguata. Troels Oerting, primo capo del Centro EC3, ha dato una puntuale sintesi dei compiti dello stesso: "*Il Centro europeo per la lotta alla criminalità informatica è stato istituito per fornire competenze in qualità di centro di fusione e di centro di sostegno operativo, investigativo e forense, ma anche grazie alla propria capacità di mobilitare tutte le risorse degli Stati membri dell'UE necessarie a mitigare e ridurre le minacce provenienti dai criminali informatici, ovunque essi operino*".

In particolare, l'azione del centro segue tre direttrici:

1. Contrasto ai cybercrimes commessi da gruppi della criminalità organizzata, in particolare quelli che generano profitti illeciti ingenti, come le frodi on-line.

[12] Dopo aver condotto uno studio di fattibilità sull'istituzione del Centro: "*Feasibility study for a European Cybercrime Centre*", relazione finale, febbraio 2012.

2. Contrasto ai cybercrimes che causano gravi danni alle loro vittime, come lo sfruttamento sessuale dei minori nella rete.
3. Contrasto ai cybercrimes (compresi attacchi informatici) che interessano le infrastrutture strategiche e i sistemi di informazione nell'Unione.

Sulla base di queste macroaree di intervento, sono state individuate le funzioni del Centro, che ruotano attorno a 4 pilastri fondamentali[13]:

- Fungere da punto di riferimento europeo per la diffusione e condivisione di informazioni sulla criminalità informatica.

  Il primo modo per contrastare efficacemente un'attività criminale altamente specializzata è contribuire alla conoscenza approfondita della stessa. Grazie all'istituzione di un centro unico a livello europeo, viene garantita una raccolta capillare di informazioni avente fonti pubbliche, private o accessibili al pubblico; vengono così arricchiti i dati di polizia disponibili e colmate progressivamente le lacune delle informazioni fornite dagli organismi preposti alla sicurezza informatica e alla lotta alla criminalità informatica. Le informazioni raccolte possono riguardare le attività di criminalità informatica in senso stretto, i metodi con cui tali attività vengono svolte e i loro presunti autori. Tale funzione permette di migliorare la conoscenza del fenomeno, attuare un'efficace prevenzione, rendere più celere l'accertamento e la repressione dei reati informatici e favorire lo sviluppo di legami tra autorità di contrasto, la rete delle squadre di pronto intervento informatico (CERT[14]) e gli specialisti del settore privato in materia di sicurezza delle tecnologie dell'informazione e della comunicazione (TIC).

[13] Comunicazione della Commissione UE al Consiglio e al Parlamento europeo: "*Lotta alla criminalità nell'era digitale: istituzione di un Centro europeo per la lotta alla criminalità informatica*" del 30 marzo 2012; Relazione 2014 sull'EC3 reperibile al seguente link: https://www.europol.europa.eu/content/european-cybercrime-center-ec3-first-year-report

[14] I CERT (*Computer Emergency Response Team*) sono squadre che si pongono come punto di riferimento in rete per la risposta ad emergenze informatiche di qualsiasi genere. Il primo centro di questo tipo nacque nei primi anni '90 su impulso della statunitense Defense Advanced Research Projects Agency (DARPA) allo scopo di assistere gli utenti della rete in caso di incidente informatico, prevenire eventuali futuri incidenti e promuovere una cultura a livello internazionale sulla sicurezza informatica. I team sono composti da esperti informatici e si occupano di varie attività, in particolare di informazione, formazione, supporto e assistenza tecnica, ricerca e sviluppo. Ad oggi esistono varie squadre non solo in Italia ma anche nel mondo (CERT nazionale Italia dal 2014, PI-CERT di Posteitaliane, CERT-DIFESA presso il Ministero di Difesa; RUS-CERT a Stoccarda, US-CERT presso il Dipartimento di Sicurezza Federale del governo USA): CERT-IT rappresenta l'Italia a livello internazionale nel FIRST

- Mettere in comune a livello europeo competenze all'avanguardia in materia di criminalità informatica per aiutare gli Stati membri a rafforzare le proprie capacità, sia a livello legislativo sia a livello operativo. L'EC3 funge da ausilio per gli Stati membri nel contrastare la criminalità informatica, sia mettendo a disposizione le proprie competenze sia organizzando specifiche attività di formazione i cui destinatari sono le autorità di contrasto e le autorità giudiziarie. Consolidando il lavoro di Europol, l'EC3 permette di creare reti di relazioni e piattaforme attive per lo scambio di informazioni con il mondo dell'industria e con altri partner non istituzionali, quali la comunità scientifica e le organizzazioni della società civile. In questo modo è reso più agevole lo scambio di informazioni tra i vari soggetti ed è possibile rendere più tempestive le segnalazioni di minacce informatiche, con una conseguente risposta collaborativa di tipo "task force" agli attacchi informatici e ad altri tipi di reati informatici. Si crea così un fondamentale "*hotspot*" per scambiare le migliori pratiche e le conoscenze in questo settore, instaurare relazioni con gli Stati membri, le autorità di contrasto internazionali, le autorità giudiziarie, il settore privato e le organizzazioni della società civile e rispondere alle loro domande, ad esempio, in caso di attacchi informatici o nuove forme di truffe online. Fondamentale è anche l'attività di formazione realizzata dal centro, che si sostanzia sia nell'acquisizione di competenze tecniche approfondite sia nel rafforzamento delle capacità delle forze di polizia, dei pubblici ministeri e dei giudici dei singoli Stati membri specificamente richieste in ambito informatico.
- Fornire sostegno tecnico-operativo agli Stati membri durante indagini riguardanti illeciti informatici e nelle operazioni di polizia, per mezzo di studi strategici, analisi operative[15], incoraggiando l'istituzione di squadre investigative comuni e facilitando lo scambio di informazioni operative nelle indagini in corso. A questo proposito, l'EC3 fornisce un'assistenza di alta qualità nell'analisi tecnica forense (strutture, archivi, strumenti) nonché

(*Forum of Incident Response and Security Teams*) consorzio nato nel 1990 grazie all'impulso di 11 CERT che oggi accorpa più di un centinaio di team di differenti nazionalità.

[15] Nell'arco del primo anno sono stati prodotti studi sul c.d. *deep web*, sulla nuova moneta virtuale (*bitcoins*) e sull'economia virtuale sommersa. Fonte: relazione primo anno di attività di EC3 (2014).

specifiche competenze di criptazione per le indagini sulla criminalità informatica.

- Rappresentare l'applicazione della legge dell'UE in settori di interesse comune, ponendosi come portavoce dell'investigazione di livello europeo nell'ambito della criminalità informatica.

Il centro è l'interfaccia naturale con le attività di Interpol sulla criminalità informatica e le altre unità internazionali di polizia preposte alla lotta contro la criminalità informatica. Collabora inoltre con organizzazioni internazionali quali la rete INSAFE alla realizzazione di campagne di sensibilizzazione, aggiornandole continuamente in risposta alle evoluzioni della criminalità informatica, al fine di promuovere un comportamento online prudente e sicuro che funga da primo ostacolo alla consumazione di reati.

Il centro è stato progettato sulla base di una struttura organizzativa semplice e snella, al fine di realizzare efficacemente la necessaria sinergia operativa che sempre deve guidare la sua azione: attraverso lo sfruttamento congiunto di abilità diversificate e strumenti all'avanguardia, EC3 cerca di garantire una forte coesione interna e una rapida comunicazione delle informazioni, anche con gli Stati membri. All'interno della suddivisione operativa di Europol, sono stati creati gruppi di analisi focalizzati su un determinato oggetto d'indagine, chiamati *Focal Points* (FP). Tre di questi lavorano nell'ambito degli scopi istituzionali di EC3[16], cui si affianca, come elemento complementare di coordinamento, il *Cyber Intelligence Team* (CIT) che migliora il loro lavoro, fungendo da collettore per i dati rilevanti provenienti dalle varie fonti, al fine di arricchire le informazioni disponibili delle forze dell'ordine degli Stati membri.

Nel primo anno di EC3, Focal Point Cyborg ha assistito gli Stati membri coordinando 19 importanti indagini di criminalità informatica e fornendo un essenziale supporto per portare a termine due grandi indagini internazionali relative ai c.d. *ransomware*[17].

[16] Il primo gruppo denominato "*Cyborg*" si occupa dei c.d. High-Tech crimes (attacchi informatici di grande portata, malware); il secondo gruppo, "*Terminal*", si occupa del mondo dell'e-commerce ed in particolare delle frodi nei pagamenti online; il terzo gruppo, "*Twins*", svolge la sua attività nell'ambito dello sfruttamento sessuale dei minori a mezzo della rete.

[17] Il *police ransomware* è un tipo di malware che blocca il computer dell'utente-vittima, accusandolo di aver visitato siti web illegali contenenti materiale pedopornografico o di aver

Nelle indagini svoltesi durante il primo anno di attività, la polizia spagnola, lavorando in stretta collaborazione con EC3 e con l'Interpol, ha condotto 11 arresti, smantellando una vasta e complessa rete di criminali informatici dedita alla diffusione del "police ransomware". Si stima che i criminali abbiano colpito decine di migliaia di computer in tutto il mondo, assicurandosi profitti al di sopra di un milione di euro per anno di attività. Nella seconda operazione sono stati condotti due arresti e sono state sequestrate versioni più recenti del malware[18] per 50.000 euro in moneta virtuale. Il supporto di EC3 alla polizia spagnola è stato molto prezioso per concludere positivamente un'altra operazione internazionale molto complessa, la quale ha bloccato la vendita dell'accesso a 21.000 server compromessi, collocati in 80 paesi, per rendere anonima la propria attività su Internet[19].

Coordinando le indagini di autorità belghe e olandesi di polizia in un'operazione volta a smantellare un gruppo di hacker dedito al *vishing*[20], l'azione di EC3 ha contribuito in modo decisivo al suo positivo esito, 12 arresti e il sequestro di più di 15.000 euro in contanti.

In una delle ultime operazioni[21] EC3 ha coordinato un'operazione internazionale congiunta che ha bloccato la botnet *Ramnit*, la quale era riuscita ad infettare 3,2 milioni di computer in tutto il mondo, al fine di rubare informazioni personali, coordinate bancarie e disabilitare le protezioni antivirus[22]. I rappresentanti di

---

compiuto altre attività illegali. Gli hacker, fingendosi addetti delle forze dell'ordine, chiedono così il pagamento di una "penale" per sbloccare il computer della vittima: l'inganno risulta efficace poiché il malware fa visualizzare sulla schermata iniziale del computer della vittima un messaggio che blocca il funzionamento dell'elaboratore, apparentemente proveniente dalle forze dell'ordine, soggetto che legittimamente indaga le attività illegali nella rete. In questo modo i cybercriminali convincono la vittima a pagare la "multa" attraverso due tipi di gateway di pagamento - virtuali e anonimi - a titolo di penale per il presunto reato commesso.

[18] Si trattava di un ransomware più aggressivo, in grado anche di crittografare i dati delle vittime, rendendo le stesse più propense a pagare il riscatto nella speranza di recuperare i loro dati.

[19] I responsabili sono stati arrestati con l'accusa inoltre di riciclaggio dei proventi illeciti derivanti dall'utilizzo del malware.

[20] Il *vishing* (voice-phishing) è un particolare tipo di frode posta in essere al fine di lucro attraverso la captazione ingannevole di dati sensibili: l'azione fraudolenta viene realizzata attraverso la comunicazione telefonica (per es. con la tecnologia VoIP) e non con l'invio di mail.

[21] Operazione Rubly dell'inizio del 2015.

[22] Le *botnets* sono reti di terminali "*zombie*", ovvero computer che sono stati silenziosamente infettati con virus o malware di qualsiasi genere e che in tal modo consentono all'utente non autorizzato o remoto il controllo degli stessi. Gli hacker hanno così la piena disponibilità di strumenti informatici pronti ad "infettare" altri devices; il collegamento di vari computer in una rete crea la possibilità di attacco in più direzioni, rendendo il lavoro nel complesso nettamente

diversi Paesi e partner del settore privato sono stati strettamente coinvolti, riuscendo così a chiudere la rete di comando delle micro botnet che si erano create, i server di controllo e infine reindirizzando 300 domini Internet utilizzati dai controllori del circuito infetto.

Il Focal Point Terminal fornisce supporto investigativo alle agenzie UE di contrasto alle frodi nei pagamenti internazionali, agevolando la collaborazione tra le forze dell'ordine, il settore privato e le autorità di regolamentazione. In particolare, è uno dei principali partner di lavoro per garantire la sicurezza e la fiducia dei clienti nei pagamenti elettronici e on-line all'interno di un mercato in rapida crescita come è quello telematico. Le analisi, la raccolta di informazioni e il supporto riguardano sia frodi perpetrate attraverso l'utilizzo materiale della carta sia quelle operazioni fraudolente poste in essere grazie alla mera conoscenza dei codici collegati al conto corrente o alla carta di credito di un determinato utente; inoltre, l'azione di FB Terminal è rivolta altresì agli attacchi agli ATM o ai sistemi POS attraverso i c.d. *skimmer.*

Nel 2013, Focal Point Terminal ha fornito supporto operativo e analitico per 29 importanti operazioni internazionali, che hanno portato allo smantellamento di 3 grandi reti di produzione e diffusione di carte di pagamento false[23].

FP Terminal crea prodotti di analisi e facilita la cooperazione tra gli attori di cui sopra, al fine di combattere la frode pagamento crimine in tutto il mondo.

Le sfide maggiori che EC3 affronta per l'avvio e il coordinamento efficace delle operazioni sono spesso legate all'incapacità di ricevere direttamente le prove decisive dall'industria privata: in altri termini, il funzionamento effettivo di EC3 è ancora ostacolato dal livello di sottosegnalazione dei casi di reati informatici registrato dalle forze dell'ordine, probabilmente per paura di danni d'immagine.

---

più rapido e più redditizio. Dal 2007 le botnets sono diventate la forza dominante nella produzione e distribuzione di "*spam*", nonché di vari tipi di "*phishing*": infatti, nel 2008 le botnets risultano le responsabili della diffusione di circa il 90% di tutte le mail "spam".

[23] Un'operazione ha portato all'arresto di 29 persone che erano riuscite a guadagnare 9 milioni di euro sottraendo le credenziali di 30.000 titolari di carte di credito. Nella seconda operazione sono stati condotti 44 arresti (seguiti ad altri 15 arresti precedenti; 59 arresti in totale) e sono stati sequestrati due workshop illegali per la produzione di dispositivi e di software per manipolare i terminali POS. Apparecchiature elettroniche illegali, dati finanziari, carte clonate e contanti sono stati sequestrati durante 82 perquisizioni domiciliari in Romania e in Regno Unito, con il coinvolgimento di più di 400 agenti di polizia. Il gruppo aveva colpito circa 36 000 soggetti, fra titolari di carte di credito e titolari di conti correnti in 16 paesi europei.

Non avendo il quadro completo della portata lesiva degli illeciti e delle tendenze nell'ambito della criminalità informatica, l'operato di EC3 nelle forme del coordinamento investigativo e operativo, nella formazione e nella produzione di analisi e strategie risulta difficoltoso. Questo impedisce altresì la condivisione delle informazioni sulle minacce con l'industria privata al fine di proteggere tempestivamente i sistemi informatici e telematici.

6.1.4. *Cybercrime Repository* (UNODC)

Anche le Nazioni Unite hanno affrontato il problema della criminalità informatica in chiave preventiva, attraverso la centralizzazione e condivisione di informazioni rilevanti. È così nato il progetto di una banca dati unica al mondo, che raccoglie casi giurisprudenziali di 181 Stati, la legislazione rilevante, con l'accesso ai testi completi e le *best practices* in materia di lotta al cybercrime.
L'Ufficio delle Nazioni Unite per la lotta alla droga e al crimine, a margine della sessione della Commissione sulla prevenzione del crimine e la giustizia penale di maggio 2015, ha lanciato e messo a disposizione di tutti un database, il *cybercrime repository*, unico nel suo genere[24], con l'obiettivo di combattere il cybercrime, condividendo informazioni e conoscenze rilevanti. In tal modo viene favorita la cooperazione tra Stati con l'obiettivo di prevenire il verificarsi o il ripetersi degli illeciti informatici.
Soggetti pubblici e privati possono attingere ad un insieme potenzialmente enorme di informazioni, da cui possono derivare utili suggerimenti per le strategie da adottare a livello statale o da parte della singola impresa.
Al momento del lancio dell'iniziativa, Loide Lungameni, capo del Dipartimento che si occupa della criminalità organizzata, ha osservato che questo nuovo database è l'unico strumento attualmente disponibile a livello globale che contiene le leggi, i casi e le lezioni apprese sulla criminalità informatica: "*Il repository consente ai legislatori di attingere alla banca dati della legislazione nella redazione di leggi sulla criminalità informatica o per assumere prove*

[24] Il database è disponibile a quest'indirizzo: https://www.unodc.org/cld/index-cybrepo.jspx

elettroniche, facilita la cooperazione internazionale, aiutando le forze dell'ordine e pubblici ministeri ad individuare disposizioni legislative sugli illeciti informatici applicabili in altri Stati, ed offre agli utenti esempi di buone pratiche nella prevenzione, nelle indagini e nel perseguimento dei cybercrime."

Il repository, la cui consultazione è semplice ed intuitiva, si compone di tre parti che mirano a facilitare gli sforzi degli Stati membri delle Nazioni Unite *'uniti contro la criminalità informatica*':

- Il database *Legislation* si pone come collettore della legislazione sostanziale e processuale relativa agli illeciti informatici e alla prova elettronica di 181 paesi, ed è consultabile per Paese, tipo di illecito informatico e disposizioni relative agli aspetti procedurali. Il database consente agli utenti di accedere sia ad estratti di leggi, con la trattazione specifica di questioni trasversali, sia a documenti legislativi completi;
- Il *Case Law* database contiene i casi giurisprudenziali e i dati relativi alle operazioni di contrasto, sulla criminalità informatica e sui reati inerenti alla prove elettroniche. Questo permette agli utenti di vedere in che modo i vari Stati affrontano casi di criminalità informatica sia durante le indagini sia nel momento del procedimento penale;
- Il *Lessons Learned* database che contiene le prassi nazionali, le best practices e le strategie adottate a livello nazionale per prevenire e combattere la criminalità informatica. Anche in questo caso, l'intento è quello di rendere conoscibili a chiunque si interessi quelle pratiche che hanno condotto a risultati positivi sia nel settore pubblico sia nel settore privato[25].

L'Italia è stato uno dei primi Paesi ad inserire dei testi di legge, casi giurisprudenziali e report sulle iniziative intraprese: tuttavia l'effettivo impatto di tale lodevole iniziativa internazionale deriverà dal livello di collaborazione che saprà promuovere da parte dei singoli Stati firmatari, non sussistendo nessun obbligo di contributo in capo agli stessi.

[25] Le informazioni inserite in questo database sono state raccolte nel quadro dello studio globale promosso dall'UNODC sulla criminalità informatica.

6.2 Le iniziative in Italia

Negli ultimi anni anche il nostro Paese ha saputo muoversi nella direzione del contrasto alle frodi informatiche: il crescente impatto economico-finanziario di tali attacchi ha fatto maturare negli attori pubblici e privati la consapevolezza della necessità di escogitare metodi e strumenti volti alla prevenzione del danno causato al singolo utente e di riflesso a tutta la collettività.

Le iniziative degne di nota nel settore pubblico hanno riguardato da un lato la protezione delle infrastrutture strategiche attraverso l'istituzione di un Centro *ad hoc*, dall'altro i settori delle frodi nell'uso degli strumenti di pagamento alternativi al denaro contante e, più recentemente, i furti d'identità: per contrastare detti fenomeni, si è scelto di potenziare l'apparato informativo di cui dispongono le imprese e, in generale, tutti gli stakeholders, creando dei *Data-base* che consentano di verificare se una determinata transazione sia perfezionata con metodo di pagamento valido, da persona legittimata ovvero realmente corrispondente alla persona fisica agente. Altro importante intervento, riguardante però solo le frodi aventi ad oggetto finanziamenti europei, si sostanzia nella realizzazione di uno strumento informatico nazionale integrato per la condivisione di dati rilevanti.

Sicuramente questi sistemi informativi hanno il pregio di diffondere fra gli attori del settore indicazioni essenziali relative a situazioni "sospette" che altrimenti rischierebbero di rimanere negli archivi delle singole società: la condivisione di informazioni permette di aumentare la conoscenza di tutti e di creare perciò una rete di *guardians*[26] informali, capace di bloccare all'origine ogni tentativo di frode senza che debba intervenire l'apparato pubblico; inoltre risulta essenziale per l'elaborazione di strategie operative realmente efficienti nonché per

[26] In criminologia, molte teorie analizzano il ruolo dei cc.dd. *guardians*, soggetti che si pongono in una relazione di protezione – anche involontaria – rispetto al bene di volta in volta tutelato: in particolare, alcuni studi (Cohen e Felson, 1979, in materia di prevenzione situazionale) hanno dimostrato che in determinate ipotesi l'assenza dei *guardians* è elemento fondamentale per la decisione di delinquere o meno. Da tali studi emerge come, nel momento in cui tutti i soggetti appartenenti ad un determinato contesto si pongono come controllori rispetto al bene considerato meritevole di protezione, si creino le condizioni per abbattere il rischio criminale: chiunque decida di delinquere dovrà fare i conti con maggiori rischi di essere scoperto e quindi sanzionato, rimanendo invariata l'appetibilità del bene target.

diffondere fra gli utenti un senso di affidabilità rispetto all'utilizzo delle nuove tecnologie nelle transazioni. Tuttavia si rileva fin da subito qualche criticità, ovvero la frammentarietà di detti interventi e la povertà d'azione dal punto di vista della diffusione di conoscenze e della sensibilizzazione nell'uso domestico delle tecnologie informatiche. Ciò può risultare un punto di debolezza, poiché l'utenza domestica viene lasciata sola e manca il coordinamento a monte per creare un'efficace azione di prevenzione a valle per lo meno con riguardo alle imprese. Le singole azioni non solo non si occupano di fornire protezione e conoscenze ai privati, ma non guardano altresì al fenomeno della frode nella sua globalità: si concretizzano in soluzioni settoriali che affrontano ogni fattispecie concreta in maniera a sé stante. In questa direzione va la creazione delle due banche dati prima citate: la scelta di istituire due archivi, l'uno per le frodi nei pagamenti e l'altro per fronteggiare i furti d'identità, gestiti da due apparati distinti, cozza con l'unicità che spesso caratterizza la materialità del fenomeno, il quale nella maggior parte dei casi si snoda in una prima fase nella quale viene sottratta l'identità altrui per poi poterla sfruttare in un secondo momento, legandola ad una carta di credito o debito falsa. È da auspicare la creazione di una banca dati integrata che permetta di avere un quadro generale del fenomeno e di avere a disposizione tutte assieme le informazioni che possono risultare rilevanti.

Per quanto riguarda le frodi informatiche di diverso tipo non esistono ad oggi archivi di dati condivisi attraverso una struttura centralizzata: senza dubbio la diffusione e condivisione di informazioni andrebbe agevolata in tutti gli ambiti in cui può consumarsi la frode, sia attraverso basi di dati per gli addetti sia con la formazione e diffusione di conoscenze di livello base per tutti gli utenti della rete.

6.2.1. Il C.N.A.I.P.I.C.[27]

Il Centro Nazionale Anticrimine Informatico per la Protezione delle

[27] https://www.commissariatodips.it/profilo/cnaipic.html

Infrastrutture Critiche (C.N.A.I.P.I.C.) è una particolare struttura di polizia incaricata in via esclusiva della prevenzione e della repressione degli illeciti informatici, di matrice comune, organizzata o terroristica, che hanno come obiettivo le cc.dd. *infrastrutture critiche informatizzate*, vale a dire tutti quegli impianti tecnologici che svolgono funzioni di rilevanza nazionale con l'ausilio di sistemi informatici o telematici[28] [29].

Anche se di fatto già operante dal 2005 come unità specializzata nel settore costituita all'interno della struttura della Polizia postale e delle comunicazioni, il C.N.A.I.P.I.C. è stato istituito formalmente con decreto del Capo della Polizia il 7 agosto del 2008, in esecuzione del decreto del Ministro dell'Interno del 9 gennaio 2008[30].

Il Centro è stato definito "una sorta di 113 privilegiato"[31] che provvede a ricevere, elaborare e trasmettere informazioni e dati relativi al funzionamento delle infrastrutture critiche, avvalendosi della stretta collaborazione delle principali società che erogano e gestiscono i servizi di primaria importanza legati all'energia (ENI), alle telecomunicazioni, alla finanza e alle reti dei trasporti di beni e persone; la sicurezza, la continuità e la rapidità delle comunicazioni sono assicurate dall'utilizzo di collegamenti telematici esclusivi e

[28] Il progetto di creare un centro *ad hoc* in grado di difendere le "infrastrutture critiche" ed affrontare in maniera adeguata le possibili minacce verso le stesse era stato elaborato per la prima volta all'interno del D.L. n. 144/2005 (c.d. decreto Pisanu), concepito per fronteggiare i problemi e i rischi legati allo sviluppo del terrorismo internazionale. Nel gennaio del 2008 il progetto ha iniziato ad avere più concretezza attraverso l'individuazione delle infrastrutture da sottoporre a maggiore tutela da parte delle forze dell'ordine.

[29] L'individuazione delle infrastrutture critiche informatizzate si è avuta con il Decreto del Ministro dell'Interno 9 gennaio 2008: "*art. 1.1. Ai sensi e per gli effetti dell'art. 7-bis del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, sono da considerare infrastrutture critiche informatizzate di interesse nazionale i sistemi ed i servizi informatici di supporto alle funzioni istituzionali di: a) Ministeri, agenzie ed enti da essi vigilati, operanti nei settori dei rapporti internazionali, della sicurezza, della giustizia, della difesa, della finanza, delle comunicazioni, dei trasporti, dell'energia, dell'ambiente, della salute; b) Banca d'Italia ed autorità indipendenti; c) società partecipate dallo Stato, dalle regioni e dai comuni interessanti aree metropolitane non inferiori a 500.000 abitanti, operanti nei settori delle comunicazioni, dei trasporti, dell'energia, della salute e delle acque; d) ogni altra istituzione, amministrazione, ente, persona giuridica pubblica o privata la cui attività, per ragioni di tutela dell'ordine e della sicurezza pubblica, sia riconosciuta di interesse nazionale dal Ministro dell'interno, anche su proposta dei prefetti - autorità provinciali di pubblica sicurezza*".

[30] Il centro trova sede dal 23 giugno 2009 a Roma in via Tuscolana, presso il Polo Tuscolano del Dipartimento della pubblica sicurezza.
https://it.wikipedia.org/wiki/Centro_nazionale_anticrimine_informatico_per_la_protezione_delle_infrastrutture_critiche

[31] D. Vulpiani, "*La nuova criminalità informatica. Evoluzione del fenomeno e strategie di contrasto*", in Rivista di Criminologia, Vittimologia e Sicurezza Vol. I, n. 1, Gennaio-Aprile 2007.

protetti, con cui si crea un vero e proprio filo diretto fra centrale ed imprese.
L'azione del C.N.A.I.P.I.C. si concretizza in primis nel funzionamento 24 ore su 24 e 7 giorni su 7 di una sala operativa dedicata all'interscambio di informazioni: è stato così creato un unico e fondamentale punto di contatto dedicato da un lato alle infrastrutture critiche, dall'altro ad ogni altro attore, anche di livello internazionale, impegnato nella protezione delle stesse.
La piena operatività del Centro è soddisfatta attraverso lo svolgimento di altre due importanti funzioni: l'una di "intelligence" e l'altra di studio ed analisi.
Gli operatori del settore di "intelligence" si occupano della raccolta dei dati e delle informazioni utili a fini preventivi, non soltanto attraverso il costante monitoraggio internet, le attività d'indagine in rete – anche sotto copertura – e le intercettazioni di comunicazioni informatiche preventive[32], ma anche in virtù dei consolidati rapporti di collaborazione operativa e condivisione informativa con gli altri corpi di polizia, gli enti e le aziende impegnati nei settori dell'ICT Security, sia a livello nazionale che internazionale[33]. L'azione di analisi si sostanzia nell'approfondimento in chiave comparativa dei dati e delle informazioni raccolte e nella predisposizione di report previsionali sull'evoluzione della minaccia, delle vulnerabilità e delle tecniche criminali, che possono riguardare i singoli sistemi gestiti dalle infrastrutture critiche ovvero la globalità degli stessi. Fornisce altresì un prezioso ausilio in termini di risorse tecniche e di personale altamente specializzato nella risposta investigativa al verificarsi di un evento criminale in danno delle infrastrutture critiche.
L'azione del Centro è completata da un settore Tecnico, deputato alla gestione ed al controllo del funzionamento dell'infrastruttura tecnologica e dei collegamenti telematici con le I.C. convenzionate, che devono sempre essere perfettamente sicuri e riservati. Si occupa inoltre dei processi di individuazione, testing ed acquisizione di risorse strumentali ed alla pianificazione di cicli di formazione/aggiornamento del personale.
Senza dubbio la struttura rappresenta un valore aggiunto nel panorama della

[32] L'art. 7 bis c. 2 della legge n. 155 del 31/07/2005, di conversione del D.L. n. 144/2005.
[33] Il C.N.A.I.P.I.C. infatti si pone come punto di contatto nazionale della Convenzione di Budapest del 2001, e altresì punto di contatto del *Network 24/7 High Tech Crime* del G8 – Gruppo Roma-Lione – per le emergenze di carattere informatico.

protezione delle infrastrutture critiche ed è degna di nota la scelta di creare un collettore specializzato in grado di funzionare in autonomia centralizzando la protezione operativa e la prevenzione degli illeciti informatici in danno delle infrastrutture strategiche; tuttavia si rileva l'estrema settorialità della sua azione e l'assenza di un obbligo di collaborazione in capo alle infrastrutture stesse.

6.2.2. Osservatorio Sicurezza e Frodi Informatiche

Fra le iniziative private, degno di nota è l'Osservatorio Sicurezza e frodi informatiche, nato nel 2012 nell'ambito di ABILab[34] come nuovo tavolo di lavoro congiunto in materia di sicurezza nelle transazioni bancarie: si tratta di un gruppo di studio ed analisi operativa di tutto ciò che riguarda l'analisi della sicurezza in ambito bancario, con particolare attenzione alle frodi nelle transazioni e alle frodi identitarie[35]. All'osservatorio partecipano interlocutori pubblici e privati: è costituito non solo da istituti bancari ma anche da interlocutori istituzionali come la Polizia Postale e delle Comunicazioni, l'Autorità Garante per la Protezione dei Dati Personali e l'Agenzia per l'Italia Digitale. Si avvale inoltre del contributo conoscitivo di partner ICT, dell'apporto più pragmatico degli operatori nel mondo delle telecomunicazioni nonché di esperti provenienti dall'European Electronic Crime Task Force[36] (EECTF) e dal

[34] ABILab, costituito dal 2002 in forma di Consorzio, si è affermato come importante centro di ricerca ed innovazione per le banche, promosso dall'Associazione Bancaria Italiana (ABI) in un'ottica di collaborazione tra banche, aziende e Istituzioni. Lo scopo principale del Consorzio è fornire agli istituti bancari adeguato supporto nel comprendere e sfruttare i vantaggi derivanti dall'uso delle tecnologie, per poter così ottimizzare i processi interni e confezionare nuovi prodotti e servizi che rispondano alle esigenze della clientela. ABILab inoltre svolge un'azione di formazione continua, promuovendo e coordinando diverse attività di ricerca, che si svolgono in un contesto di incontro e confronto tra 180 banche e 68 partner tecnologici consorziati. Le banche possono avvalersi dell'apporto conoscitivo del consorzio in autonomia, nella piena salvaguardia dell'ambito competitivo. http://www.abilab.it/home

[35] Per un approfondimento: http://www.abilab.it/web/sicurezza-e-frodi-informatiche

[36] L'*European Electronic Crime Task Force* (EECTF) è un importante gruppo di condivisione di informazioni per la lotta al cyber-crimine, nato nel 2009 grazie ad un Accordo fra l'azienda Poste Italiane, d'intesa con la Polizia Postale e delle Comunicazioni, il Dipartimento di Pubblica Sicurezza del Ministero dell'Interno e la United States Secret Service (Agenzia governativa americana creata per prevenire e combattere le frodi finanziarie). EECTF rende possibile un'efficace cooperazione strategica pubblico-privata, con lo scopo di supportare l'analisi e lo sviluppo di best-practises per il contrasto agli illeciti informatici. https://en.wikipedia.org/wiki/European_Electronic_Crime_Task_Force; http://www.posteitaliane.it/it/innovazione/cyber_security/index.shtml

mondo della ricerca scientifica come il Politecnico di Milano.

L'Osservatorio raggruppa tutte le attività di ricerca in materia di sicurezza trattate ante 2012 da due operatori separati, la Centrale d'Allarme per Attacchi Informatici e l'Osservatorio sulla Gestione Sicura dell'Identità: con la creazione di un gruppo di lavoro unitario si è voluto promuovere l'efficienza e l'incisività dell'azione del presidio, permettendo un'operatività continua e completa nell'ambito della gestione della sicurezza bancaria e delle frodi nelle transazioni.

L'Osservatorio mantiene rapporti costanti con le principali istituzioni europee e con centri di studio nazionali e internazionali attivi in materia; in particolare, a livello nazionale è rilevante la collaborazione diretta con la Polizia Postale e delle Comunicazioni proprio per il contrasto al fenomeno del cybercrime[37].

Oltre all'organizzazione di iniziative di comunicazione e formazione in materia di sicurezza informatica rivolte a tutta la comunità degli stakeholders, nel 2014 l'Osservatorio ha operato anche in qualità di centrale d'allarme per gli attacchi informatici perpetrati nella rete Internet, grazie allo scambio informale di comunicazioni mediante la mailing list Presidio Internet ABI Lab.

Il lavoro dell'Osservatorio viene racchiuso in una rilevazione di sistema che viene presentata annualmente al convegno "Banche e sicurezza": il report è volto a valutare il posizionamento del settore bancario italiano con riguardo al livello di sicurezza nella gestione delle transazioni telematiche e delle identità virtuali, le strategie di contrasto ideate e le valutazioni di quelle tradotte in pratica[38].

6.2.3. UCAMP e SIPAF

La legge n. 166 del 17 agosto 2005[39] ha introdotto in Italia un moderno strumento di prevenzione delle frodi nel settore in continua evoluzione dei

[37] "*Intesa tra ABI e Polizia contro il crimine informatico*", 5 giugno 2015: https://www.abi.it/Pagine/news/Intesa-tra-ABI-e-Polizia-.aspx

[38] Per un approfondimento: http://www.abilab.it/web/sicurezza-e-frodi-informatiche

[39] Legge recante "*Istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento*", pubblicata in G.U. n. 194 del 22 agosto del 2005.

pagamenti virtuali. Si tratta di un sistema di prevenzione amministrativa[40] articolato attorno all'Ufficio Centrale Antifrode nei Mezzi di Pagamento (UCAMP) e al Data-base SIPAF (Sistema informatizzato per la Prevenzione Amministrativa delle Frodi sulle Carte di Pagamento), supportati e sempre aggiornati da un gruppo di lavoro interdisciplinare (GIPAF) con funzioni consultive.

L'Ufficio Centrale Antifrode nei Mezzi di Pagamento è stato costituito nell'ambito della Direzione V del Ministero del Tesoro al fine di creare un unico e stabile interlocutore con le società private che operano nel campo della sicurezza bancaria: in tal modo è possibile fungere da collettore di informazioni da parte di coloro che si confrontano quotidianamente con il fenomeno della frode in tutte le sue forme ed evoluzioni tecnologiche[41]. I costanti colloqui con gli esperti, uniti al quotidiano confronto con le società emittenti consentono di delineare il quadro generale sia dal punto di vista teorico-scientifico, sia dal punto di vista prettamente empirico, elaborando di conseguenza strategie di prevenzione efficaci e fornendo attività di formazione specialistica in ambito nazionale ed internazionale[42].

Da tali studi è emerso che la strategia migliore per prevenire il fenomeno delle frodi nell'uso delle carte di pagamento consiste nel diffondere informazioni "scottanti" fra gli addetti del settore, i quali in tal modo hanno la possibilità di riconoscere con rapidità le transazioni suscettibili di configurare un rischio di frode oggettivo ed imminente.

Proprio a tal fine è nato SIPAF, un sistema informatizzato di raccolta dati relativi

---

[40] Con la legge n. 166, il legislatore ha stabilito che le misure di "prevenzione amministrativa" da adottare nello specifico settore delle carte di pagamento rientrano tra i compiti di pubblico interesse che lo Stato è chiamato a svolgere a vantaggio della collettività. La prevenzione amministrativa in quest'ambito ha il compito di individuare i punti di criticità nei sistemi di sicurezza delle società che emettono le carte di pagamento; ideare, anche attraverso interventi di tipo legislativo, soluzioni in grado di eliminarli progressivamente, mediante una stretta collaborazione pubblico-privato; stabilire gli standard minimi, sul fronte della sicurezza, che le stesse società emittenti saranno chiamate ad osservare.
http://www.dt.mef.gov.it/it/antifrode_mezzi_pagamento/prevenzione_frodi_mezzi_pagamento/

[41] L'UCAMP trae origine dal Regolamento (CE) n. 1338/2001 che ha istituito il sistema europeo di protezione dell'Euro: la sua prima funzione infatti è stata quella di monitorare le falsificazioni in danno della moneta unica. Con la normativa italiana di attuazione (Legge n. 166/2005 e D.M. n. 112/2007) si è deciso di ampliare tali attribuzioni, inglobando quelle di prevenzione delle frodi sulle carte di pagamento e sugli strumenti dedicati all'erogazione del credito al consumo. http://www.governo.it/backoffice/allegati/76514-9625.pdf

[42] Art. 17 Decreto del Ministro dell'Economia n. 112/2007.

a transazioni sospette o a casi di utilizzo di carte false[43]. L'archivio permette di condividere le informazioni riguardanti situazioni finanziarie caratterizzate da alto rischio di frode, le quali altrimenti rimarrebbero in possesso delle singole società emittenti; vengono altresì segnalate le conseguenti ricadute sui punti di accettazione degli strumenti di pagamento, siano essi esercizi commerciali (POS) o distributori ATM.

Gli enti segnalanti sono tutti gli attori che partecipano alla vita del settore delle carte di pagamento, perciò sia le società, le banche e gli intermediari finanziari emittenti, sia coloro che gestiscono reti commerciali di accettazione di dette carte[44]. Il Data-base è composto da due sezioni, l'una dedicata ai *dati*, intesi come segnalazioni di eventi di danno già perfettamente consumati, oggettivi e consolidati relativi ai c.d. sconvenzionamenti[45], ai punti di vendita riconvenzionati, alle transazioni disconosciute dai titolari delle carte ed infine agli sportelli automatici (ATM) manomessi[46]; l'altra relativa alle *informazioni*, nella quale vengono inserite le segnalazioni d'allerta relative a potenziali sospetti di frode in corso, ovvero fatti non ancora consolidati in corso di monitoraggio da parte degli enti segnalanti[47].

Sulla base dell'analisi dei dati estratti dal SIPAF viene redatto annualmente il Rapporto statistico sulle frodi con le carte di pagamento, con il quale è possibile capire i trend del settore nel lungo periodo, anche attraverso un'analisi comparata con Paesi europei ed extraeuropei dei risultati ottenuti, nonché valutare l'impatto concreto in termini economici e di risultato delle strategie adottate. Il rapporto ha cadenza annuale e prevede un annesso riservato destinato agli enti segnalanti e alle istituzioni (Banca d'Italia, Magistratura, Forze di Polizia)[48]. La pubblicazione ha lo scopo di fotografare la realtà italiana

[43] https://sipaf.tesoro.it/SIPAF/faces/xhtml/protected/home.xhtml
[44] Art. 1 l. 166/2005 e artt. 2-3-10-11 del Decreto del Ministro dell'Economia n. 112/2007.
[45] Si parla di sconvenzionamento quando viene revocata la convenzione ad un Point of Sales (POS) precedentemente abilitato alle transazioni elettroniche.
[46] Art. 6 del D.M. n. 112/2007.
[47] Art. 7 del D.M. n. 112/2007: affinché possa ritenersi sussistente la situazione d'allerta devono essere rispettati i parametri stabili in via generale ed astratta all'art. 8 dello stesso Decreto.
[48] Nel rapporto pubblico vengono riportati i risultati delle analisi in forma aggregata e in percentuale, mentre nell'annesso riservato le stesse informazioni appaiono nei loro valori assoluti e con un grado di dettaglio molto più elevato. Rapporto statistico n. 4/2014 al link: http://www.governo.it/backoffice/allegati/76514-9625.pdf

in materia di frodi legate alle carte di pagamento, in modo da diffondere a livello generale la conoscenza della portata del fenomeno e dell'attività svolta dall'UCAMP: in questo modo si vuole rendere più consapevole e informato l'utente consumatore medio, incentivandolo conseguentemente ad utilizzare gli strumenti di pagamento elettronico.

Fondamentale per l'azione di intelligence nell'ambito delle frodi è la convenzione del 2012 stipulata tra il Ministero dell'Economia e delle Finanze e il Ministero dell'Interno per l'accesso telematico al SIPAF. Questo accordo ha previsto la possibilità per selezionati ed abilitati utenti delle forze di polizia di accedere in via telematica ai dati e alle informazioni contenuti nell'archivio informatizzato[49]. L'accesso alla banca dati da parte delle forze di polizia avviene nel pieno rispetto della Privacy ed è limitato *ex lege* alle finalità di prevenzione e repressione dei reati connessi o comunque collegati all'utilizzo di carte di credito o di altri mezzi di pagamento. Tale collaborazione risulta perciò estremamente utile, poiché permette alle forze di polizia di avere a disposizione in tempo reale una grande quantità di dati ed informazioni utili provenienti direttamente dagli addetti del settore.

Anche la Banca d'Italia collabora con l'Ufficio Antifrode, fornendo informazioni aggiornate e dettagliate sulle transazioni.

6.2.4. SCIPAFI[50]

Visti i positivi risultati cui l'approccio preventivo ha condotto nel campo degli abusi nell'utilizzo di carte di credito e pagamento, l'art. 33 lett. d-ter) della Legge n. 88/2009 ("legge comunitaria 2008")[51] ha previsto l'istituzione presso il Ministero dell'Economia e delle Finanze di un Sistema Pubblico di Prevenzione, sul piano amministrativo, delle frodi nel settore del credito al consumo e dei pagamenti dilazionati o differiti, con specifico riferimento al furto d'identità.

[49] Ai sensi dell'art. 7 L. n. 166/2005 e del D.M. 112/2007 di esecuzione.
[50] http://www.dt.tesoro.it/it/antifrode_mezzi_pagamento/furto_identita/
[51] Fra le fonti comunitarie recepite, rileva specificamente l'attuazione della Direttiva CE 2008/48 relativa ai contratti di credito al consumo.

L'attuazione del dettato legislativo è avvenuta nel 2011 con il D.lgs. n. 64[52], il quale ha istituito un sistema di prevenzione simile nell'articolazione organizzativa a quello realizzato pochi anni prima in materia di antifrode nell'uso degli strumenti di pagamento elettronico: anche in questo caso infatti si è prevista l'istituzione di un archivio centrale informatizzato e di un gruppo di lavoro, di supporto e gestione dello stesso.[53]

Tuttavia, a differenza di SIPAF gestito direttamente in ambiente ministeriale, per il contrasto al furto d'identità si è deciso di scorporare la fase operativa dalla titolarità dell'archivio: la realizzazione e la gestione del Data-base sono stati affidati a Consap S.p.A., mentre la titolarità del sistema rimane assegnata in via esclusiva al Ministero dell'Economia e delle Finanze[54].

L'accesso alla banca dati SCIPAFI consente il raffronto delle informazioni contenute nei principali documenti d'identità, riconoscimento e reddito, con quelli registrati nelle banche dati degli enti di riferimento, attualmente quelle dell'Agenzia delle Entrate, Ministero dell'Interno, Ministero delle Infrastrutture e dei Trasporti, INPS e INAIL: l'accesso è garantito 365 giorni all'anno 7 giorni su 7[55]. Tale riscontro si configura come efficace strumento di prevenzione per i "furti d'identità" intesi sia come impersonificazioni totali sia parziali ed assolve altresì alla funzione di deterrente, essendo numerosi i casi nei quali gli aderenti hanno l'obbligo di consultazione e rimanendo sempre possibile la ricerca facoltativa; si crea così una rete telematica nella quale gli aderenti, condividendo informazioni che altrimenti rimarrebbero riservate, aumentano la conoscenza diffusa del fenomeno e conseguentemente l'incisività della risposta preventiva. Ognuno ha sempre a propria disposizione informazioni relative ai

---

[52] D.lgs. n. 64 dell'11 aprile 2011, "*Ulteriori modifiche ed integrazioni al decreto legislativo 13 agosto 2010, n. 141, per l' istituzione di un sistema pubblico di prevenzione, sul piano amministrativo, delle frodi nel settore del credito al consumo, con specifico riferimento al furto d'identità*": tale decreto ha aggiunto il titolo V bis al D.lgs. n. 141/2010 in considerazione dell'omogeneità della materia.

[53] Il gruppo svolge funzioni di coordinamento, impulso e indirizzo per l'individuazione e l'attuazione delle strategie di prevenzione delle frodi identitarie; stabilisce inoltre le linee guida per l'elaborazione, sotto il profilo statistico, dei dati contenuti nell'archivio centrale. http://www.consap.it/fondi-e-attivita/supporto/furto-d-identita

[54] I rapporti fra la concessionaria e l'ente pubblico sono disciplinati da apposita Convenzione stipulata il 22 luglio 2013.

[55] Al seguente link è possibile visualizzare la mappa del sistema: http://www.dt.tesoro.it/it/antifrode_mezzi_pagamento/furto_identita/sistema_prevenzione.html

furti d'identità avvenuti o anche solo tentati nei confronti di tutti i membri della rete, che in tal modo hanno la possibilità di capire dove si annidano le criticità dei propri sistemi ed elaborare le strategie operative più efficienti.

Il sistema tuttavia presenta criticità nel contrastare le frodi perpetrate mediante l'utilizzo di identità fittizie o create mescolando ad arte elementi di fantasia e dati di persone fisiche realmente esistenti o esistite[56].

L'accesso al Sistema, disciplinato dal Titolo V bis integrato nel D.lgs. 141/2010 con modalità individuate nel Regolamento attuativo[57], è attualmente previsto in via obbligatoria per banche, comprese quelle europee ed extraeuropee, intermediari finanziari, fornitori di servizi di comunicazione elettronica, fornitori di servizi interattivi o servizi ad accesso condizionato e dal 16 luglio 2015 anche per le compagnie di assicurazione: costoro sono definiti "aderenti diretti" e hanno il dovere di consultare il sistema per richieste relative a dilazioni o differimenti di pagamenti, finanziamenti o servizi a pagamento differito, se il cliente non ha avuto precedenti rapporti diretti con il soggetto aderente, né risulta essere una persona la cui identità è nota allo stesso[58].

I gestori di sistemi di informazione creditizia e le imprese che offrono servizi assimilabili alla prevenzione delle frodi possono aderire al sistema tramite apposita convenzione con il MEF: vengono identificati come "aderenti indiretti" e possono accedere solo previo conferimento di delega da parte degli aderenti diretti, previo parere conforme del Garante per la protezione dei dati personali.

Il concreto funzionamento del sistema si articola in tre moduli funzionali:

- Il modulo Interconnessione di rete, attraverso il quale vengono tradotte in input d'accesso alla banca dati SCIPAFI le richieste di verifica provenienti dagli aderenti: avvenuta l'elaborazione, il software restituisce l'output, positivo o negativo, relativo alla verifica effettuata;
- Il modulo Informatico di Allerta, che raccoglie le segnalazioni di frodi subite o di rischio di frode provenienti dai soggetti aderenti nonché gli alert

[56] http://www.consap.it/fondi-e-attivita/supporto/furto-d-identita

[57] Decreto MEF del 19 maggio 2014 in vigore dal 16 luglio 2014. Per le fonti di riferimento: http://www.dt.tesoro.it/it/antifrode_mezzi_pagamento/furto_identita/normativa.html

[58] Al seguente link è possibile consultare la lista degli aderenti diretti autorizzati: http://www.dt.tesoro.it/export/sites/sitodt/modules/documenti_it/prevenzione_reati_finanziari/prevenzione_reati_finanziari/Lista_aderenti_diretti_autorizzati_24_03_2015.pdf

generati dal titolare dell'archivio per rendere edotti gli stessi aderenti di situazioni di particolare pericolosità;

- Il modulo Informatico centralizzato, il quale funziona da vero e proprio collettore di dati: raccoglie infatti in modo aggregato e anonimo informazioni relative sia alle richieste di verifica dell'identità che hanno dato esito negativo, sia alle frodi subite. Questo modulo permette al Ministero e al Gruppo di lavoro[59] lo studio di una moltitudine di informazioni provenienti da soggetti diversi, al fine di comprendere il fenomeno del furto d'identità nel suo complesso e i suoi modi di manifestarsi e di svilupparsi nel tempo in relazione a diversi profili di analisi (quali il territorio, il settore economico, ecc.), il suo impatto, la sua percezione.

Si prevede inoltre che l'accesso al sistema sia consentito alle forze di polizia, nonché agli uffici del Dipartimento della pubblica sicurezza del Ministero dell'interno competenti in materia di analisi dei fenomeni criminali e di cooperazione, anche internazionale, all'Unità di informazione finanziaria della Banca d'Italia e al Nucleo speciale di polizia valutaria della Guardia di finanza[60].

[59] Nel gruppo sono rappresentati, oltre al Ministero dell'economia e delle finanze, il Ministero dell'interno, il Ministero della giustizia, il Ministero dello sviluppo economico, la Banca d'Italia e la Guardia di Finanza. Manuale operativo di SCIPAFI (2015): http://www.dt.tesoro.it/export/sites/sitodt/modules/documenti_it/prevenzione_reati_finanziari/prevenzione_reati_finanziari/Manuale_operativo_15_gennaio_2015.pdf

[60] Art. 20 D.M. n. 95 del 19 maggio 2014.

Capitolo VII: la frode informatica nell'ordinamento giuridico spagnolo

Il delitto di frode informatica (*estafa informatica*) è stato introdotto nell'ordinamento giuridico spagnolo con la Ley organica n. 10 del 23/11/1995, di promulgazione del nuovo codice penale[1]. Non si trattò di un intervento ad hoc in materia informatica come avvenne in Italia, bensì di una legge di riforma complessiva del sistema penale, con la quale si volle rispondere a tutte le nuove esigenze di tutela, incluse quelle emerse con lo sviluppo tecnologico degli anni Novanta: in particolare, negli anni del codice penale previgente i tribunali si erano spesso trovati in difficoltà nel giudicare casi di trasferimenti virtuali fraudolenti di somme di denaro, manipolazioni di dati bancari al fine di far risultare crediti inesistenti o debiti estinti, poiché non esisteva alcuna disposizione volta a sanzionare nello specifico tali condotte. Il codice penale del 1944, più volte riformato, rimaneva ovviamente il risultato dello sviluppo economico-tecnologico coevo, perciò il primo ostacolo alla sua applicazione in ambito informatico era la mancata previsione nelle singole fattispecie incriminatrici della possibilità di ledere beni virtuali o immateriali, cionondimeno dotati di valore economico: i delitti posti a tutela del patrimonio prevedevano tutti come oggetto della condotta beni materiali o valori economicamente misurabili, dotati di una certa corporeità[2].

Altro ostacolo nei casi sopraindicati era la mancanza nei fatti di un rapporto *intuitu personae* e del fondamentale requisito dell'induzione in errore della persona offesa: su questo problema sia la dottrina spagnola sia quella italiana si sono interrogate a lungo, in via maggioritaria sostenendo fosse difficile applicare il delitto di truffa (*estafa*[3]), poiché si riteneva comunemente che la

[1] Si tratta del codice penale oggi vigente in Spagna, promulgato dal Re Juan Carlos I al fine di adeguare pienamente l'ordinamento giuridico ai principi dello stato sociale e democratico positivizzati all'interno della Costituzione del 1978. Con esso fu sostituito il codice previgente del 1944, prodotto della Guerra Civile, che era stato più volte riformato nel tentativo di renderlo più adeguato all'assetto democratico. I continui ritocchi snaturarono l'impianto complessivo e resero necessaria l'emanazione di un codice completamente nuovo, perfezionato solo nel 1995. La riforma più importante del nuovo codice è del 2010, con la Ley organica n. 5 del 22/06/2010, la quale modificò buona parte dei delitti previsti, incluso il delitto di *estafa*. https://es.wikipedia.org/wiki/C%C3%B3digo_Penal_de_España; https://rodas5.us.es/file/17b47490-8c07-7430-6566-b19c2a8f511c/1/leccion1_SCORM.zip/pagina_01.html

[2] M. Gonzáles Suárez, "*Fraudes en Internet y Estafa Informatica*", Trabajo fin de Master, Universidad de Oviedo, Mayo 2014.

[3] Art. 248.1 Código Penal.

fattispecie tradizionale fosse un caso esemplare di "bilateralità necessaria", in cui sussiste sempre una relazione fra due persone, colui che inganna (in Italia colui che pone in essere gli artifici e raggiri) e colui che conseguentemente cade in errore e, per ciò stesso, pone in essere un atto di disposizione patrimoniale per sé pregiudizievole. In particolare, la dottrina maggioritaria spagnola ha sempre sostenuto come l'induzione in errore sia elemento essenziale ed autonomo nel delitto di *estafa*, in grado di delimitare i confini dell'inganno rilevante ai fini della tipicità e di fornire il parametro per la valutazione della colpevolezza.

Nei casi di utilizzo di uno strumento tecnologico al fine di procurarsi un'utilità economica, anche i giuristi iberici non riuscivano a superare l'ostacolo dell'interlocutore automatizzato: infatti si sosteneva comunemente l'impossibilità di ingannare una macchina, la quale si limita sempre e solo ad eseguire i comandi impartiti[4].

La giurisprudenza si è mostrata tendenzialmente aderente a questo indirizzo interpretativo, pur dimostrando attenzione prioritaria alle esigenze di giustizia sostanziale e conseguentemente forzando a volte i principi di legalità e tipicità: si registrano sentenze in cui si è ritenuto sussistente il delitto di *estafa* tradizionale bypassando nelle motivazioni il problema dell'inganno della vittima, proprio al fine di non lasciare impunite condotte palesemente lesive di beni giuridici rilevanti. Nei casi in cui negavano la qualificazione giuridica in termini di *estafa*, i giudici cercavano comunque di giungere ad una condanna argomentando sulla base di altre disposizioni incriminatrici, come il delitto di appropriazione indebita o il delitto di malversazione di fondi pubblici, nel caso in cui sussistesse la qualifica di funzionario pubblico[5].

---

[4] O. Morales García in "*Principios de derecho de la sociedad de la información*", Aranzadi, Thomson Reuters, 2010, cap. 13. Per un approfondimento del dibattito in Italia: par. 2.2.

[5] Tribunal Supremo (STS) del 19 aprile 1991 (RJ 1991, 2813): nella fattispecie, i giudici negano la qualificazione in termini di *estafa* e ritengono sussistente il delitto di *apropriación indebida* nella condotta di inserimento fraudolento nell'elaboratore di dati contabili per il trasferimento illecito di denaro dei correntisti. La qualificazione finale si è basata sulla sussistenza nel caso concreto del vincolo di amministrazione che legava il soggetto attivo alla disponibilità dell'accesso ai conti correnti dei clienti: perciò se lo stesso fatto fosse stato posto in essere da un *extraneus*, non vi sarebbe stata alcuna disposizione penale applicabile. Tribunal Supremo (STS) del 30/10/1998 (RJ 1998, 8566): il giudice supremo cassa la sentenza di merito che qualificava come *estafa* il fatto del funzionario pubblico che introduce dati falsi nel database previdenziale, al fine di far ricevere a degli amici pensioni pubbliche non spettanti, ritenendo

Ad ogni modo, era pacifica l'insufficienza delle norme penali vigenti per fronteggiare tali fenomeni criminali.

La riforma del 1995 ha colmato la lacuna, portando sicuramente chiarezza nel panorama applicativo, ed ha ampliato il novero delle condotte penalmente rilevanti strutturando la disposizione relativa al reato di truffa in due commi, il primo dedicato alla *estafa clásica*, il secondo dedicato alla specificazione di modalità assimilate, la *estafa informatica* e gli atti preparatori: l'obiettivo principale non era sanzionare la specifica – ma per certi versi astratta – categoria dei delitti informatici, bensì colpire le condotte fraudolente poste in essere in ambito bancario da coloro che hanno per ragioni professionali la disponibilità di terminali e possono in tal modo realizzare trasferimenti fraudolenti di somme depositate sui conti correnti. Si è così introdotto l'art. 248.2 lett. a) cod. pen. il quale stabilisce quanto segue: "*También se consideran reos de estafa: a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro*[6]*".*

Basandosi sulla scelta di posizionare la norma all'interno dell'articolo dedicato alla *estafa*, la dottrina maggioritaria sostiene ancor oggi che si tratti di una "truffa impropria" o una "truffa generica", rilevando come sussistano delle caratteristiche che rendono difficile una completa equivalenza con il reato tradizionale di cui al comma 1[7].

Risulta subito evidente come la collocazione sistematica della fattispecie differisca da quella operata dal legislatore italiano del 1993: da un lato, il codice penale spagnolo contempla, all'interno dell'articolo dedicato al reato di truffa, un comma specifico per sanzionare – considerandole espressamente vere e

---

invece sussistenti gli estremi del delitto di *malversación de caudales públicos*, pur esplicitamente affermando che il funzionario non aveva la disponibilità sull'oggetto materiale della condotta per ragioni d'ufficio.

[6] "*Si considerano altresì colpevoli del delitto di truffa: a) coloro che, con intento di lucro e avvalendosi di una manipolazione informatica o di un artificio simile alla stessa, ottengano un trasferimento non autorizzato di attivo patrimoniale in danno altrui*".

[7] G. Balmaceda Hoyos, "El *delito de estafa informática en el derecho europeo continental*", in Revista de Derecho y Ciencias Penales N. 17, 2011, Universidad San Sebastián (Chile); J. García García-Cervigón, "*El fraude informático en España e Italia – Tratamiento jurídico-penal y criminológico*", in "Revista cuatrimestral de las Facultades de Derecho y Ciencias Economicas y Empresariales", n. 74, mayo-agosto 2008.

proprie ipotesi di truffa[8] – le condotte fraudolente derivanti da "*manipolazioni informatiche o artifici simili*", dimostrando così il legislatore di voler colmare il vuoto normativo attraverso l'individuazione di condotte assimilabili alla truffa che comportassero l'ampliamento dei confini della punibilità della condotta tradizionale (art. 248.1 cód. pen.). In altri termini, si voleva fornire una risposta penale adeguata ad un fenomeno percepito dalla collettività come sostanzialmente truffa, ma che in realtà non integrava l'elemento tipico essenziale del delitto anzidetto: senza l'inganno causativo di errore non si potevano considerare esistenti né una truffa né una frode di qualche genere[9]. Anche la scelta di non inserire nel nuovo comma una sanzione specifica denota l'intento di introdurre nel sistema una *species* di truffa, attribuendo con certezza legislativa illiceità penale a delle condotte che si porrebbero ai limiti dell'interpretazione estensiva. Ai casi di condotta realizzata con "*manipulación informatica*" risulta applicabile l'arsenale sanzionatorio previsto per la classica truffa nonché, se sussistono i requisiti, tutte le relative aggravanti.

Una parte della dottrina si è mostrata fin da subito critica con l'opzione legislativa, sostenendo che sarebbe stato più corretto creare una figura di reato autonoma, ma comunque plaudendo all'integrazione[10].

Dal canto suo, il legislatore repubblicano italiano non è mai stato in grado di attuare una riforma completa del sistema penale emanando un nuovo codice: gli interventi normativi del Dopoguerra sono stati settoriali e specifici, alcuni modificativi del codice penale, altri strutturati in micro-sistemi *extra codicem*, ma tutti tendenti a rispondere alle contingenti istanze della collettività. Anche nel caso della criminalità informatica il legislatore si è mosso in questo modo: ritenendo che fosse un fenomeno meritevole di attenzione specifica, ne ha analizzato le peculiarità e le analogie rispetto alle vigenti previsioni e infine ha scelto di emendare il codice penale attraverso una legge speciale[11] che andava

[8] È la formulazione stessa della norma a segnalarlo: il comma 2 esordisce con "*tambien son reos de estafa los que*" ("sono altresì colpevoli di truffa coloro che"), dimostrando di voler considerare a tutti gli effetti ipotesi di truffa i casi elencati alle lettere a), b) e c).

[9] M. Gonzáles Suárez, "*Fraudes en Internet y Estafa Informatica*", Trabajo fin de Master, Universidad de Oviedo, Mayo 2014

[10] Suárez Gonzáles, en R. Mourullo (dir.)/J. Barreiro (coord.), "*Comentarios al Código Penal*", Madrid: Editorial Civitas, 1997.

[11] La più volte citata Legge n. 547 del 23 dicembre 1993.

ad emendare ciascun titolo, rispettando la sistematica ispirata alla lesione del bene giuridico. L'art. 640-ter c.p. è stato inserito nel codice penale subito dopo il delitto di truffa e appare come fattispecie autonoma: ciononostante il legame con la fattispecie tradizionale è stato presto messo in evidenza sia da parte della dottrina, che lo ha conseguentemente annoverato fra le *species* del delitto di cui all'art. 640 c.p., sia dalla giurisprudenza maggioritaria, che fin dalle prime sentenze ha ritenuto utilizzabili anche per i casi di frode informatica gli esiti interpretativi relativi ai concetti di danno e profitto di cui all'art. 640 c.p.[12].

Se è vero che, nella sostanza, l'applicazione del delitto di frode informatica in Italia ha scontato per molti anni la vicinanza concettuale con la fattispecie di truffa, è pur vero che la scelta del legislatore italiano, formalmente opposta alla parallela opzione spagnola, ha conferito alla norma enormi potenzialità: infatti, la scelta di collocare in una fattispecie ad *hoc* le frodi informatiche ha permesso più recentemente di legittimare quegli esiti interpretativi che più si allontanano dalla fenomenologia della classica truffa, nei quali i giudici hanno sottolineato l'autonomia concettuale dell'illecito informatico rispetto all'art. 640 c.p. con il quale condivide solo aspetti di contorno. Inoltre ha creato le opportune premesse per l'inserimento di aggravanti speciali inerenti alla natura e alla fenomenologia della lesione informatica, come il furto o indebito utilizzo di identità digitale e il fatto commesso da operatore di sistema.

La *estafa* informatica, come anche la fattispecie italiana, è pacificamente un delitto posto a presidio del patrimonio (alcuni, per la verità pochi in dottrina la considerano a tutela dei sistemi informatici): lo dimostrano la collocazione sistematica all'interno della fattispecie di truffa e la *voluntas legis* sottesa a tale scelta di punire testualmente "trasferimenti di attività patrimoniali", caratterizzati dall'assenza di un'apprensione fisica o materiale della somma, e perfezionati solamente con un'alterazione contabile dei dati inerenti alla situazione patrimoniale di un correntista.

Per quanto riguarda la disposizione italiana, pur risultando evidente e condivisa nella dottrina maggioritaria la sua natura di delitto contro il patrimonio, nondimeno si pone come efficace presidio anche per altri beni giuridici, come la

[12] Per un approfondimento: cap. II par. 2,6.

trasparenza e la sicurezza degli scambi nella rete e l'integrità dei sistemi informatici e telematici[13]. Inoltre la possibilità di introdurre delle aggravanti speciali ha permesso di ampliare la portata del presidio penale includendovi beni giuridici come la riservatezza informatica nel riferimento all'identità digitale e il legittimo affidamento tutelato nella qualifica di chi ricopre il ruolo di operatore di sistema.

Dal punto di vista della struttura del reato, fra le due norme sussistono somiglianze e differenze: entrambe sono costruite come reati d'evento, che si consumano perciò con la effettiva lesione del bene giuridico contemplato. Ma, mentre nella disposizione italiana l'evento è individuato nel conseguimento di ingiusto profitto con altrui danno, nella disposizione spagnola il riferimento è al "*trasferimento non autorizzato di attività patrimoniali*": perciò per il diritto spagnolo non è necessario, ai fini della consumazione del reato, che l'agente consegua la materiale disponibilità della somma frodata, essendo sufficiente la realizzazione all'interno del sistema informatico del trasferimento non autorizzato. La disposizione italiana è più vaga, esprimendosi nei termini di "procurarsi un profitto": risulta infatti controverso in dottrina e giurisprudenza se l'agente debba avere la materiale disponibilità del profitto – come dovrebbe concludersi considerando la frode informatica una mera *species* di truffa – oppure se risulti sufficiente che la persona offesa non abbia più signoria sul bene e contemporaneamente l'agente si trovi nella situazione di poterne fruire in via esclusiva e immediata.

Sicuramente la disposizione spagnola risulta più precisa, poiché la condotta è penalmente rilevante solo se conduce causalmente ad un trasferimento non autorizzato di attività patrimoniali: allo stesso tempo però emerge la natura della norma pensata e voluta a tutela di interessi prettamente economici, dato che il concetto di "*trasferimento non autorizzato di attività patrimoniali*" risulta più specifico e per ciò stesso più limitato rispetto a quello italiano di profitto, con potenzialità applicative di tipo meramente patrimoniale ristrette agli ambiti bancario, assicurativo e commerciale.

Se, nell'interpretazione della disposizione italiana, si optasse per la necessità

[13] Per un approfondimento: cap. II par. 1.

della materiale apprensione del profitto da parte dell'agente, la consumazione del delitto italiano interverrebbe in un momento cronologicamente successivo rispetto a quella del corrispondente spagnolo, posto che sarebbe necessaria la prova dell'apprensione materiale dell'utilità patrimoniale o del denaro frodato. Il vantaggio della contestazione del delitto spagnolo sarebbe evidente in quelle ipotesi in cui non è possibile provare la materiale apprensione del denaro frodato da parte dell'agente, magari perché avviene all'estero o perché si colloca a notevole distanza di tempo.

Si potrebbe ravvisare nell'*eventus damni* del delitto spagnolo una vicinanza concettuale con l'evento intermedio individuato in Italia da una parte della dottrina nella causazione di un risultato irregolare nel processo di elaborazione dei dati, cui segue causalmente il profitto con danno altrui: la scelta del legislatore spagnolo di riferirsi a "*transferencia*" e non ad una "*disposición patrimonial*" sta proprio ad indicare che il delitto risulta perfettamente consumato anche senza l'intervento umano, solo con l'operazione automatica dell'elaboratore.

La condotta tipica è descritta sia nella disposizione italiana sia nella disposizione spagnola in termini di clausola generale, lasciando quindi al diritto vivente il compito di riempirla di significato[14]. La tipizzazione italiana risulta però più completa, poiché si esprime con termini più tecnici: all'alterazione del funzionamento di un sistema informatico o telematico o intervento senza diritto su dati, informazioni o programmi corrisponde in Spagna una "*manipulación informatica o artificio semejante*". Tale concetto risulta potenzialmente molto ampio e alcuni in dottrina lo ritengono stridente con il principio di legalità[15]: infatti non si fa riferimento ad una condotta manipolativa che colpisca direttamente il funzionamento dell'elaboratore, facendogli compiere una certa operazione in modo diverso rispetto a com'era stato originariamente programmato, bensì risulta penalmente rilevante qualsiasi tipo di manipolazione realizzata in ambito informatico. In dottrina si definisce diffusamente il concetto

[14] G. Balmaceda Hoyos, "*El delito de estafa informática en el derecho europeo continental*", in Revista de Derecho y Ciencias Penales N. 17, 2011, Universidad San Sebastián (Chile).
[15] J. García García-Cervigón, *op.cit.*; J. Antonio Choclán Montalvo, "*Fraude informático y estafa por computación*", en "Internet y Derecho penal", Cuadernos de Derecho Judicial, (X-2001).

di manipolazione informatica nei termini di "*azione che supponga un intervento nel sistema informatico, alterando, modificando o occultando i dati che devono essere trattati in maniera automatizzata, ovvero modificando le istruzioni di programma, al fine di alterare il risultato prestabilito dell'elaborazione informatica*"[16]: senza dubbio sono quindi comprese tutte le manipolazioni di input (introduzione di dati falsi nel sistema ovvero alterazione, soppressione o occultamento di dati precedentemente introdotti), di programma o di output (alterazione del prodotto dell'elaborazione automatizzata) compiute su *software*; risulta più complesso includervi le alterazioni di *hardware*, assimilabili maggiormente al delitto di *daño* (danneggiamento)[17].

Si può notare che la formula per certi versi indeterminata adottata dal legislatore è stata concretizzata a livello dottrinale con una definizione molto vicina alla tipizzazione normativa italiana: vengono considerate manipolazione informatica sia l'alterazione del funzionamento di un programma sia l'intervento fraudolento sui dati oggetto dell'elaborazione.

Stante la molteplicità delle modalità in cui potrà essere realizzata la *manipolación informatica*, ciò che – secondo l'interpretazione più accreditata – deve sempre essere valutato con rigore, anche ai fini della valutazione della colpevolezza dell'agente, è l'effettiva idoneità dello strumento utilizzato ad operare il trasferimento di attivo patrimoniale[18]: questo aspetto permette di avvicinare concettualmente il secondo e il primo comma del delitto dell'art. 248 cód. pen., realizzando un parallelismo fra la concreta capacità dello strumento utilizzato di perfezionare il trasferimento fraudolento di denaro e l'idoneità dell'inganno ad indurre in errore la persona offesa.

Nel precetto spagnolo viene contemplata una seconda modalità d'offesa, ovvero l'utilizzo di un "*artificio semejante*" (artificio simile) rispetto alla manipolazione informatica: si tratta di una formula che non trova un corrispondente nella disposizione italiana e che ha fatto molto discutere la dottrina spagnola, divisa fra coloro che la ritengono una utile formula di

[16] J. García García-Cervigón, *op.cit*.
[17] Il delitto di daño può concorrere con la frode informatica anche in quei casi di manipolazione sul software in cui i dati vengono distrutti o resi completamente inservibili.
[18] O. Morales García, *op.cit*.

chiusura, in grado di includere nell'alveo applicativo della *estafa informatica* quelle condotte non caratterizzabili pienamente come manipolazioni informatiche[19], e coloro che la criticano in quanto troppo indeterminata, perciò lesiva del principio di tipicità legale[20].

La posizione di coloro che in Spagna guardano con favore alla generale formula, scelta dal legislatore del '95 proprio al fine di sanzionare quelle manipolazioni aventi come destinatario immediato macchine automatizzate non considerabili propriamente "informatiche", trova un corrispondente italiano nelle recenti applicazioni giurisprudenziali dell'art. 640-ter c.p. a casi di manomissione di *slot machine*: nell'ordinamento spagnolo, l'opzione non è stata lasciata alla prassi applicativa ma è stata effettuata a monte, con la previsione di una clausola ampia in grado di ospitare ogni tipo di manipolazione anche solo similare a quelle informatiche, includendovi le ipotesi di manomissioni di macchine dal funzionamento automatizzato, *id est* distributori di benzina, di cibi o bevande al fine di ottenere un ingiusto vantaggio; in Italia, invece, tale risultato è stato – parzialmente – raggiunto grazie all'iter interpretativo svolto nei tribunali sul concetto di "sistema informatico o telematico", nel quale sono state comprese la macchine da gioco a vincita aleatoria.

La genericità della formula "*artificio semejante*" ha permesso alle corti iberiche di avvallare un'interpretazione molto libera della nozione, criticabile dal punto di vista del principio di tipicità, ma in grado di dare una risposta alle concrete esigenze di tutela derivanti da situazioni di indubbio disvalore sociale ma senza un riscontro in una disposizione penale specifica: sono le ipotesi di uso illegittimo di carte di credito o debito e il fenomeno del c.d. phishing. La giurisprudenza ha comunque sempre tentato di limitare la potenzialità applicativa di questa modalità commissiva chiedendo anche in questo caso la prova dell'effettiva idoneità del mezzo a realizzare il trasferimento fraudolento[21].

L'utilizzo illegittimo di strumenti di pagamento non ha trovato tipizzazione

[19] J. Córdoba Roda, M. García Arán, "*Comentarios al Código Penal, parte especial*", Aranzadi, 2004.
[20] O. Morales García, *op.cit*.; Suárez Gonzáles, en R. Mourullo (dir.)/J. Barreiro (coord.), *op.cit*.
[21] G. Balmaceda Hoyos, "*El delito de estafa informática en el derecho europeo continental*", in Revista de Derecho y Ciencias Penales N. 17, 2011, Universidad San Sebastián (Chile).

specifica nel codice penale spagnolo fino alla riforma del 2010[22]: la prima soluzione adottata dal legislatore si è avuta con la redazione del codice penale vigente ma risultò poco soddisfacente, poiché si trattava di una interpretazione autentica del concetto di *llave falsa* (chiave falsa), strumento per commettere il delitto di *robo con fuerza* (rapina): si consideravano *llaves falsas* le carte di credito a banda magnetica e quelle perforate, senza l'aggiunta di alcuna formula più generica in chiusura[23]. In tale delitto però non erano sussumibili le condotte tipiche in cui si sostanzia l'uso fraudolento di strumenti di pagamento, vale a dire il prelievo allo sportello automatico senza il consenso del titolare e l'utilizzo della carta negli esercizi commerciali convenzionati, a causa del requisito tipico dell'accesso al *luogo* dove le cose oggetto di rapina si trovano: inoltre la mancanza di una formula aperta lasciava fuori dal novero delle "*llaves falsas*" le carte a microchip, che oggi sono le più diffuse[24]. Ne derivava un problematico vuoto di tutela, colmato per via giurisprudenziale applicando proprio il delitto di *estafa informatica*, sulla base di una supposta equivalenza fra sostituzione di persona di fronte allo sportello automatico e *artificio semejante*[25].

Come accennato, il problema fu risolto in sede legislativa nel 2010, andando a modificare l'art. 248. 2 cod. pen. con l'aggiunta di una nuova lett. c) dove si stabilisce che [sono altresì colpevoli di truffa] "*Los que, utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero*"[26]*.* Ancora una volta il legislatore spagnolo ha scelto di ampliare i confini della truffa tradizionale, includendovi attraverso la certezza della norma positiva qualsiasi tipo di operazioni fraudolente commissibili attraverso l'utilizzo di strumenti di pagamento, titoli di viaggio ovvero soltanto i dati inerenti gli stessi,

[22] Ley organica n. 5 del 22/06/2010
[23] O. Morales García, *op.cit*.
[24] Il problema era acuito dal fatto che il Tribunale Supremo, con una pronuncia del 2002, aveva ritenuto integrato il delitto di falso in moneta di cui all'art. 387 cód. pen. nella manipolazione della banda magnetica dello strumento di pagamento: Pleno no jurisdicional, Sala Segunda, 28/06/2002.
[25] Tribunal Supremo (STS) sentencia del 20/11/2001 (RJ 2002, 805); O. Morales García, *op.cit*.
[26] "*Coloro che, utilizzando carte di credito o debito, titoli di viaggio, o i dati inerenti a qualsiasi di questi, pongano in essere operazioni di qualsiasi tipo in danno del titolare o di terzi*".

senza l'autorizzazione del titolare[27]. Il panorama viene poi completato da un'altra disposizione, che sanziona qualsiasi alterazione, copia o riproduzione fraudolenta, la mera detenzione di strumenti di pagamento falsi, nonché l'utilizzo in danno altrui da parte di colui che non ha partecipato alla falsificazione ma ne è a conoscenza[28].

Il corrispondente illecito italiano, posto in una legge speciale e non nell'impianto codicistico, si differenzia da quelli spagnoli soprattutto per un aspetto contenutistico, vale a dire l'unicità del riferimento normativo: con un'unica fattispecie è possibile sanzionare tutti gli utilizzi fraudolenti degli strumenti di pagamento, inclusi gli atti preparatori e gli abusi da parte del titolare.

Anche il "phishing" è stato ricondotto dall'orientamento interpretativo maggioritario al delitto di *estafa informatica*, per il tramite della condotta che si avvale degli "*artificios semejante*": a proprio sostegno, costoro sottolineano che si tratta della fattispecie che meglio rispetta la fenomenologia dell'attacco informatico in commento, data l'insussistenza di una relazione fra l'agente e la vittima e la realizzazione dell'atto di disposizione patrimoniale da parte di quest'ultima sulla base di un artificio che ha come destinatario immediato l'elaboratore. Questa è l'impostazione anche della giurisprudenza di merito maggioritaria nonché del Tribunale Supremo, il quale è giunto così ad inglobare nel concetto di "*artificios semejantes*" qualsiasi condotta che richieda meccanismi informatici per la realizzazione e termini in un'appropriazione indebita[29]. Chi critica tale approccio rileva come non si possa realmente considerare sussistente una manipolazione simile a quella informatica nell'atto della "pesca di dati", risolvendosi questo nell'impiego di tecniche di ingegneria sociale che puntano a creare per la persona offesa un contesto non corrispondente al vero: infine, si sottolinea come manchi il nesso causale diretto fra condotta manipolativa ed evento lesivo, poiché il risultato dell'azione non

[27] Permane comunque il riferimento alle carte di pagamento con banda magnetica e alle carte perforate nella fattispecie di robo con fuerza; O. Morales García, *op.cit*..

[28] Art. 399-bis cód. pen.

[29] Alcune sentenze hanno ritenuto che sia da verificare un requisito tacito, vale a dire il fatto che l'artificio posto in essere attraverso lo strumento informatico abbia indotto in errore la persona offesa: sent. A.P. Soria 00016/2012 de 27 de febrero. Per la qualificazione giuridica in termini di "phishing": Tribunal Supremo (STS) Sentencia de 12/06/2007 (RJ 2007, 3537); Tribunal Supremo (STS) Sentencia 8284/2012 de 25/10/2012. Sala de lo Penal. Sección Primera. N. de Recurso: 2422/2011. N. de Resolución: 834/2012. Ponente: Manuel Marchena Gómez.

integra il trasferimento fraudolento richiesto nella *estafa informatica*, bensì comporta una mera captazione di dati, grazie alla quale è poi il soggetto agente a frodare successivamente il denaro[30]. In altri termini, l'agente non altera in alcun modo dati, programmi o sistemi informatici ma pone in essere un mero inganno attraverso l'elaboratore, avvicinandosi così la condotta alla tipizzazione contemplata nella classica *estafa*.

Per la verità, la natura giuridica di quella che abbiamo precedentemente definito la "fase 1" del phishing[31] ha incontrato solo isolate opinioni contrarie in dottrina; ciò che invece ha fatto dibattere a lungo teorici e pratici del diritto è la qualificazione giuridica della c.d. fase 2, il momento dell'intervento de "*los muleros bancarios*"[32]. Gli esiti interpretativi della dottrina e giurisprudenza spagnole sono per certi aspetti diversi da quelli raggiunti in Italia, poiché ritengono prevalentemente che integri gli estremi della *estafa informatica* anche il comportamento di colui che si presti a prelevare materialmente il denaro per poi ritrasferirlo, essendo sufficiente, ai fini dell'applicazione della fattispecie in commento, che costui sia consapevole dell'illiceità della provenienza del denaro[33]. Per l'opinione dominante spagnola, non è necessaria la prova del fatto che il *mulero* fosse consapevole della consumazione di una specifica frode informatica: siccome egli partecipa attivamente alla consumazione del reato "a monte", non gli può essere contestato il reato di ricettazione, il quale richiede la mancanza di partecipazione al delitto da cui deriva il provento illecito trasferito dall'agente. Si ammette però in via del tutto residuale la contestazione del delitto di *Blanqueo de capitales por imprudencia grave* (riciclaggio di denaro con grave negligenza) ex art. 301.3 cód. pen., nel caso in cui non si abbia la prova del dolo – anche solo eventuale – nella realizzazione del reato a monte[34].

In Italia, si è visto come recenti pronunce della giurisprudenza di merito abbiano

---

[30] O. Morales García, *op.cit*.

[31] Per l'analisi del "phishing" cap. V par. 3.

[32] Il "*mulero bancario*" è la figura denominata comunemente "*financial manager*", colui che accetta una fasulla offerta di lavoro su Internet consistente nell'ospitare una somma di denaro sul proprio conto corrente ovvero per prelevare la somma e trasferirla nuovamente all'estero. Per approfondire l'argomento, cap. V par. 3.

[33] Tribunal Supremo (STS) sentencia de 12/06/2007, EDJ 2007/70163; 16/03/2009, EDJ 2009/134682; 25/10/2012, EDJ 2012/279319.

[34] http://www.elderecho.com/penal/Phising-Problematica-calificacion-participacion-jurisprudencia_11_533680004.html

distinto a seconda che il c.d. *financial manager* sia consapevole genericamente della illiceità della provenienza del denaro che acconsente a trasferire od ospitare sul proprio conto ovvero sappia specificamente della previa consumazione di una frode informatica e accetti di collaborare[35].

Nel primo caso non potrà essergli contestato il delitto di cui all'art. 640-ter c.p., bensì potrà essere imputato dei reati di ricettazione o riciclaggio, sussistendo nella fattispecie concreta tutti gli elementi tipici: soltanto nel secondo caso potrà essere mossa la contestazione dello specifico reato posto in essere "a monte", poiché altrimenti difetterebbe l'elemento soggettivo, essendo indubbio che non si può muovere un rimprovero verso un soggetto per un fatto del quale non conosce gli elementi costitutivi.

Anche il sistema della perseguibilità risulta differente: mentre in Italia si è scelto di mantenere per l'ipotesi base la perseguibilità a querela e solo per le ipotesi aggravate l'intervento *ex officio*, l'ordinamento iberico ha optato per la generale perseguibilità d'ufficio ma raggiungendo una certa deflazione del carico giudiziario con la previsione della sola pena pecuniaria per le condotte meno gravi, vale a dire i casi nei quali il profitto rimane al di sotto della soglia dei 400 euro.

Pregio della disciplina spagnola è sicuramente il sistema di sanzioni predisposto per gli illeciti penali, che garantisce più effettività sia nella comminazione della sanzione sia nella incisività della stessa rispetto alla condizione economica del condannato: viene stabilita la soglia di 400 euro del profitto per individuare le condotte di minor lesività, per le quali viene comminata la pena pecuniaria (*multa*) "*de uno a tres meses*", da quantificare nel caso concreto con il sistema delle quote[36]. Per le ipotesi in cui il profitto superi i 400 euro si stabilisce in generale la pena detentiva da 6 mesi a 3 anni,

[35] Il riferimento corre a due sentenze di merito del 2013: per un approfondimento, cap. V par. 3.

[36] Il sistema delle quote assomiglia al metodo di quantificazione della pena introdotto in Italia nel 2001 per le persone giuridiche. In Spagna, viene utilizzato anche per le persone fisiche, permettendo di commisurare la sanzione alle effettive capacità economiche del reo e connotarla così di concreta effettività afflittiva; a livello generale, la disposizione incriminatrice prevede una *multa* che va da un minimo ad un massimo quantificato non già in denaro ma in mesi, permettendo di garantire così il principio di eguaglianza di tutti i cittadini di fronte alla legge. La quantificazione concreta avviene in sede applicativa da parte dell'autorità giudiziaria: ad ogni giorno possono corrispondere dai 2 euro ai 400 euro e la valutazione avviene esclusivamente sulla base delle condizioni economiche del reo.

da quantificare sulla base dei criteri previsti all'art. 249 cod. pen.: vengono poi elencate all'art. 250 cod. pen. delle ipotesi di *estafa* considerate particolarmente gravi, per le quali si prevedono cumulativamente la pena detentiva da 1 a 6 anni e la multa da 6 a 12 mesi.

Conclusioni

L'attenzione richiesta agli operatori del diritto in ambito informatico è sempre più alta, essendo milioni le persone che quotidianamente rimangono vittime di accessi abusivi, frodi, virus e malware di ogni genere, senza che intervenga una efficace tutela in grado di ripristinare lo status quo ante o, per lo meno, ripianare la perdita e punire i responsabili. Probabilmente ciò è dovuto in primis alle difficoltà applicative insite nella fattispecie incriminatrice di cui all'art. 640-ter c.p. e, più in generale, alle criticità del nostro sistema repressivo: oltre ai problemi di tipo dogmatico-interpretativo, si ha una sanzione pecuniaria poco deterrente, una sanzione privativa della libertà poco o nulla attinente alla fenomenologia dell'offesa e che per vari meccanismi spesso non viene concretamente scontata ed infine una estrema difficoltà di emersione delle frodi, le quali in molti casi non vengono portate a conoscenza dell'autorità giudiziaria, oppure non riescono ad essere provate in maniera esaustiva ovvero trovano giustizia troppo tardi rispetto all'evento di danno, a causa dei malfunzionamenti e degli alti costi dell'apparato processuale italiano.

Molte difficoltà verosimilmente dipendono dalla diffidenza del mondo della dottrina penalistica all'interpretazione lata delle fattispecie incriminatrici, per il timore di sfociare in una violazione del divieto di analogia *in malam partem*, unita alla ancora limitata formazione informatica del giurista: sicuramente il canone di legittimità dell'intervento penale sopracitato è fondamentale per la realizzazione dei principi dello Stato di diritto nelle aule di giustizia, tuttavia è necessario comprendere come in ambito informatico – e più in generale nel mondo delle tecnologie più evolute – l'interpretazione estensiva delle fattispecie penali sia assolutamente fondamentale per adeguare la positivizzazione legislativa ai traguardi della tecnologia: solo attraverso un ampliamento in sede interpretativa delle disposizioni incriminatrici saldamente ancorato al fatto tipico ed ai principi fondamentali del sistema è possibile rimediare a quell'ontologico ritardo che caratterizza l'introduzione delle fattispecie incriminatrici, riuscendo così ad attualizzare disposizioni già vigenti nell'ordinamento che a prima vista possono sembrare superate.

Nel caso della frode informatica, un'interpretazione lata degli elementi costitutivi appare necessaria: le scelte operate in sede di creazione della norma, consistenti per lo più in concetti generali ma sufficientemente tecnici come "*alterazione del funzionamento*", "*intervento senza diritto*" ovvero "*sistema informatico o telematico*", rispecchiano la volontà di creare una disposizione adatta a resistere al divenire dello sviluppo tecnologico e di conferire un ruolo pregnante ai protagonisti della fase applicativa della norma, evitando di ingessare in maniera eccessiva il loro compito.

Pertanto le scelte redazionali nella norma, facendo salvo per un momento il problema del coordinamento con fattispecie limitrofe come l'art. 55 c. IX del D.lgs. 231/2007, appaiono adeguate e a ben vedere lungimiranti; invero la soluzione italiana del '93 è risultata in perfetta coerenza con l'art. 8 della Convenzione Cybercrime del 2001. Il legislatore era consapevole di non poter cristallizzare in una norma positiva tutte le molteplici modalità di frode, perciò ha scelto – in questo caso a ragione – di delegare al giudice un ruolo innovatore sulla base però di clausole di partenza precise e al tempo stesso elastiche.

In quest'ambito, la funzione dei pratici del diritto corre spesso "sul fil di lana": il rischio di analogie contra reo è elevato, ma la causa è soprattutto una mancanza spesso di conoscenze tecniche del fenomeno.

L'opzione di attribuire la titolarità delle indagini e la competenza della fase preliminare all'autorità giudiziaria distrettuale non ha per ciò stesso risolto il problema, anzi sotto alcuni aspetti lo ha acuito: in Italia esistono sì realtà di prestigio come il *pool* che si occupa di reati informatici presso la procura di Milano, tuttavia si tratta di un'iniziativa interna e che ancora non risulta particolarmente diffusa altrove. Ciò che risulta criticabile – e che denota una scarsa conoscenza di base – è la legittimazione a livello legislativo dell'idea per la quale la formazione in ambito informatico non sia richiesta a tutti gli operatori del diritto ma sia prerogativa delle sedi distrettuali e possa fungere da criterio dirimente per una eccezione alle normali regole di individuazione della competenza.

Per contrastare in maniera efficace questi fenomeni e prevenire lo sviluppo di forme d'attacco sempre più invasive, è necessario incentivare ad ogni livello

sociale una conoscenza profonda della rete, delle sue potenzialità e dei rischi sottesi ad un suo uso poco accorto: in particolare, all'operatore del diritto è richiesto un considerevole sforzo conoscitivo del fenomeno informatico prima che giuridico, al fine di dominare la tecnica e sfruttarla nel lavoro di *law enforcement* e di successiva repressione. La scelta di molti governi di aumentare spesso in maniera indiscriminata la cornice edittale per le fattispecie caratterizzate da un particolare background tecnologico denota l'ancoraggio ad una concezione di diritto penale che trova la propria forza deterrente solamente nella severità della sanzione, nonché la paura della tecnica stessa, guardata con sospetto proprio a causa della limitata formazione in proposito.

Solamente una conoscenza specifica e approfondita del mondo informatico può condurre l'interprete a comprendere quando un comportamento in apparenza magari avulso dalla fattispecie in commento, in realtà integri tutti gli elementi tipici: in altri termini, l'operatore del diritto deve essere in grado di cogliere la sussistenza della condotta alterativa o interventiva sul sistema anche nelle ipotesi in cui il contesto dell'azione non è quello tradizionale. Come il mondo informatico è soggetto a rapida evoluzione, così anche l'interpretazione del diritto in ambito informatico deve essere in grado di progredire pur rimanendo salda alle proprie radici: è necessario individuare il giusto equilibrio fra il rispetto dei principi dell'ordinamento penale e la necessità di rispondere in maniera effettiva alle sempre nuove istanze della società civile, le quali a volte richiedono un ripensamento delle categorie tradizionali.

Ciò avviene grazie ai principi fondamentali del sistema, in particolare quelli di offensività della condotta e materialità della lesione, i quali consentono di individuare ciò che funge da minimo comune denominatore fra le condotte di frode, quel nucleo di offensività che si può riscontrare in tutte le diverse manifestazioni di condotta illecita prescindendo dal grado di avanzamento tecnologico, dalla specifica funzione e dalla dimensione che caratterizza il singolo sistema: nella frode informatica lo si rinviene nella manipolazione del processo "legittimo" posto in essere dall'elaboratore automatizzato o nell'intervento senza facoltà legittima sui contenuti dello stesso (con danno e profitto). La componente informatica *ex se* non può e non deve condurre

l'interprete a modificare in modo iniquo la portata della fattispecie: si tratta solamente di una τέχνη che ha permesso la creazione di un contesto del quale devono essere capite le peculiarità e le regole, al fine di reagire in modo efficace all'offesa. La componente informatica, come qualsiasi altra tecnica, è neutra: non caratterizza il fenomeno nella dimensione della lesione al bene giuridico, perciò può e deve essere sfruttata proprio per arrivare a prevenire e reprimere il crimine. I principi per risolvere in maniera conforme al diritto le questioni di tipo sostanziale ovvero processuale che si pongono in ambito informatico si rinvengono nei cardini del sistema penale, che vanno adeguati, magari integrati ma mai dimenticati.

Sicuramente grazie allo sviluppo del cyberspazio i beni giuridici tradizionali hanno subìto modificazioni anche di rilievo; secondo alcuni si può pienamente affermare che sono nati nuovi diritti specifici come la tutela della riservatezza informatica nel senso della tutela dei "*dati about oneself*" nella rete[1]. Ma il sistema penale ha molti strumenti utili per garantire tali diritti, che talora devono soltanto essere adeguati al nuovo "mondo".

Bisogna mantenere una conoscenza specifica adeguata per far vivere i principi sottesi agli ordinamenti moderni in questa nuova dimensione; e a tal fine è necessario uno sforzo collettivo che parta a livello governativo con l'investimento di maggiori risorse nella formazione e nella ricerca in campo tecnologico per ogni attore sociale, in qualsivoglia ruolo: non si tratta di conoscenze che possono rimanere nelle mani di pochi esperti.

Proprio l'interpretazione più essenzialistica e attenta alla concretezza della lesione ha permesso l'applicazione della fattispecie di frode informatica nell'ambito delle cc.dd. slot machine, che sono state considerate ai fini penali un sistema informatico-telematico. E questo percorso potrà condurre ad applicare la frode informatica ogni qualvolta la condotta fraudolenta avrà come bersaglio una macchina in grado di compiere operazioni di elaborazione dati in maniera automatizzata.

Anche la riconsiderazione del concetto di patrimonio in una prospettiva

[1] Il riferimento corre agli art. 8 CEDU e art. 7-8 della Carta dei Diritti Fondamentali dell'Unione Europea.

dinamica e in evoluzione verso una connotazione immateriale è fondamentale per adeguare il presidio introdotto nel '93 alle necessità della società contemporanea: se le prime frodi informatiche rimandavano sempre ad un danno immediatamente e facilmente quantificabile in termini economici[2], oggi accade che il guadagno – ovvero la perdita – derivante dalle condotte di manipolazione informatica abbia ad oggetto qualsiasi tipo di dato inerente ad un soggetto, non necessariamente sensibile, che nel cyberspazio risulta di facile apprensione. Già si è avuto modo di rilevare come la ricchezza sottesa allo sfruttamento dei dati inerenti ai consumatori sia potenzialmente enorme, tanto è vero che alcuni autori hanno parlato di "*oro digitale*", giacché chi ne è a conoscenza può sviluppare le strategie commerciali economicamente più efficienti: dal canto suo quindi ogni soggetto-consumatore è titolare nello spazio digitale di un bagaglio di informazioni che ha diritto di decidere come sfruttare, se divulgare, come e con chi. In questi termini è da interpretarsi il concetto di "*identità digitale*" di cui al comma terzo, il quale trova la propria collocazione ottimale in una prospettiva aperta e teleologicamente orientata: la norma di cui all'art. 640-ter c.p. diventa così un fondamentale presidio della persona, in qualsivoglia proiezione della stessa nel mondo digitale. Una legge di interpretazione autentica sarebbe sicuramente utile al fine di fare chiarezza ed indirizzare il lavoro dell'operatore del diritto, che in nessun caso può ergersi a creatore di norme penali: tuttavia, nel caso in cui il legislatore dovesse ritenere opportuno introdurre una norma definitoria dell'identità digitale, dovrebbe tenere in considerazione l'ampiezza e l'estrema fluidità del concetto stesso, evitando da un lato definizioni tautologiche o generiche, dall'altro una descrizione troppo esaustiva che finirebbe per cristallizzare una nozione, sì da renderla presto obsoleta e quindi inutile[3]. Soprattutto in ambito tecnologico, fondamentale alleato del legislatore è proprio l'interprete, che deve essere guidato con disposizioni chiare, precise e facilmente intelligibili, dai contenuti ampi ma non

[2] Ad esempio, frodi nei pagamenti, manipolazioni dati previdenziali, frodi bancarie: sono tutti casi in cui la lesione al patrimonio della persona offesa è immediatamente quantificabile in una somma di denaro.

[3] Ciò è avvenuto nel caso delle carte di credito e pagamento, nel quale la descrizione fin troppo dettagliata della fattispecie ha reso presto necessaria una forzatura interpretativa per includervi le carte a microchip. Cap. IV, par. 1.

generici. In questo senso, la scelta terminologica per la descrizione delle condotte tipiche all'art. 640-ter c.p. risulta opportuna.

La fattispecie di frode informatica così interpretata risulta una sorta di "Giano bifronte", fondamentale presidio sia sul versante personalistico della tutela del singolo nell'ambiente della rete, soprattutto alla luce del nuovo comma terzo, in ogni sua proiezione che abbia o possa avere un valore economico, sia sul versante patrimonialistico di tutela dei flussi monetari e conseguentemente della affidabilità e sicurezza dei traffici commerciali nel cyberspazio, con una connotazione pubblica se il danno ricade in capo allo Stato o ad una sua ramificazione periferica: cionondimeno, è auspicabile un intervento legislativo che unifichi in un'unica fattispecie incriminatrice le condotte incriminate dall'art. 640-ter c.p. e quelle più specifiche previste all'art. 55 c. IX del d.lgs. n. 231/2007, magari con un comma ad hoc nella disposizione codicistica che permetta di conservare le diverse condotte tipiche, l'ampiezza di tutela e il rigore sanzionatorio della disposizione di legge speciale.

Criticità della fattispecie rimane il regime di perseguibilità dell'ipotesi base unito alla tipologia e all'ammontare della sanzione: i problemi del sistema processuale penale italiano si riverberano anche nell'effettività della repressione dei casi di frode informatica, che spesso non arrivano a sentenza oppure non vengono nemmeno denunciati all'autorità competente per sfiducia e per gli alti costi. Senza soffermarsi sull'inadeguatezza della pena privativa della libertà personale per i problemi in termini di difficoltà alla rieducazione e azione criminogena del sistema carcerario italiano, si rileva come nel caso di frode informatica la sanzione più efficace ed efficiente è la sola pena pecuniaria, proprio in virtù della patrimonializzazione di ogni bene – anche inerente la persona – in ambito informatico. Sarebbe utile adottare un sistema sanzionatorio di tipo progressivo, simile a quello adottato dall'ordinamento spagnolo e in Italia per le persone giuridiche, che tenga conto di tutte le componenti del danno in ambito informatico: la sanzione pecuniaria così come fissata dal legislatore nel codice penale risulta inefficace anche nelle ipotesi aggravate, poiché in molti casi non è possibile per il giudice adeguarla al concreto danno emergente e al lucro cessante, che spesso condurrebbe ad

andare oltre il massimo previsto dalla cornice edittale. Le due categorie mutuate dal diritto civile sono estremamente utili non solo per delineare i confini del danno penalmente rilevante, ma potrebbero fornire un formidabile parametro, assieme alle condizioni economiche del reo, per la commisurazione della sanzione, al fine di renderla effettiva e adeguata ai rischi di lesione nel cyberspazio.

Alla luce di queste considerazioni, il sistema delle quote adottato in Italia per le persone giuridiche nonché quello per "*multa per dias*" ideato dal legislatore spagnolo risultano molto più efficaci ed efficienti della soluzione italiana, quindi di sicura ispirazione.

Ringraziamenti

Desidero ricordare tutti coloro che mi hanno assistito nella stesura di questo lavoro con stimolanti indicazioni, critiche costruttive ed osservazioni: a loro va il mio ringraziamento più sincero, anche se solo a me spetta la responsabilità per ogni errore contenuto in queste pagine.

Ringrazio in particolare il professor Alessandro Melchionda, relatore, ed il dott. Marco Grotto, per la grande disponibilità, attenzione e cortesia prestatami.

Proseguo con gli agenti della Polizia Postale di Trento, la sost. Proc. dott.ssa Maria Colpani e il giudice dott. Carlo Ancona che mi hanno dedicato del tempo fornendomi utili spunti per le ricerche ed interessanti materiali.

Un ringraziamento speciale va alla mia famiglia, ai miei amici e alle persone a me più care; soprattutto vorrei esprimere la mia gratitudine verso coloro che hanno speso energie e parte del proprio tempo per leggere e discutere con me le bozze del testo, supportandomi sempre con pazienza. Grazie per tutto l'interesse mostrato per il mio lavoro.

Bibliografia

Camera dei Deputati, IX Legislatura, Disegno di Legge n. 2773.
Legge n. 547 del 23 dicembre 1993, "*Modificazioni ed integrazioni alle norme del codice penale e di procedura penale in tema di criminalità informatica*" in G.U. n. 305 del 30 dicembre 1993

Convention on Cybercrime, E.T.S. No. 185 (Budapest, 23/11/2001)

D.lgs. n. 196 del 30 giugno 2003, "*Codice in materia di protezione dei dati personali*" in G.U. n. 174 del 29 luglio 2003 - Suppl. Ordinario n. 123

D.lgs. n. 82 del 7 marzo 2005, "*Codice dell'amministrazione digitale*", in nella *G.U.* n. 112 del 16 maggio 2005 - Supplemento Ordinario n. 93

D.lgs. n. 231 del 21 novembre 2007, "*Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione*", in *G.U.* n. 290 del 14 dicembre 2007- Suppl. Ordinario n. 268/L

Legge n. 48 del 18 marzo 2008, "*Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica e norme di adeguamento dell'ordinamento interno*", in G.U. n. 80 del 4 aprile 2008 - Supplemento ordinario n. 79

D.lgs. n. 141 del 13 agosto 2010, "*Attuazione della direttiva 2008/48/CE relativa ai contratti di credito ai consumatori, nonché modifiche del titolo VI del testo unico bancario (decreto legislativo n. 385 del 1993) in merito alla disciplina dei soggetti operanti nel settore finanziario, degli agenti in attività finanziaria e dei mediatori creditizi*", in G.U. n. 207 del 4 settembre 2010 - Suppl. Ordinario n. 212

Reg. UE 910/2014 del 23 luglio 2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE

D.L. n. 93 del 14 agosto 2013, convertito nella Legge n. 119 del 15 ottobre 2013, "*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*" in G.U. n. 191 del 16 agosto 2013

Decreto della Presidenza del Consiglio dei Ministri 24 ottobre 2014 "*Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale,*

nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese", in G.U. Serie Generale n. 285 del 9 dicembre 2014

D.L. n. 144 del 27 luglio 2005, "*Misure urgenti per il contrasto del terrorismo internazionale*", in G.U. n. 173 del 27 luglio 2005

Decreto del Ministero dell'Interno 9 gennaio 2008 per l'individuazione delle infrastrutture critiche di interesse nazionale, in G.U. n. 101 del 30 aprile 2008
Legge n. 166 del 17 agosto 2005 recante "*Istituzione di un sistema di prevenzione delle frodi sulle carte di pagamento*", pubblicata in G.U. n. 194 del 22 agosto del 2005

Decreto del Ministro dell'Economia e delle Finanze n. 112/2007 recante Regolamento di attuazione dell'istituzione di un sistema di prevenzione dalle frodi sulle carte di pagamento

D.lgs. n. 64 dell'11 aprile 2011, "*Ulteriori modifiche ed integrazioni al decreto legislativo 13 agosto 2010, n. 141, per l' istituzione di un sistema pubblico di prevenzione, sul piano amministrativo, delle frodi nel settore del credito al consumo, con specifico riferimento al furto d'identità*" in G.U. n. 107 del 10 maggio 2011

Decreto Ministero dell'Economia e delle Finanze n. 95 del 19 maggio 2014 in vigore dal 16 luglio 2014, in G.U. Serie Generale n. 150 del 1 luglio 2014

Dottrina

L. Alesiani, "*Il momento consumativo del delitto di frode informatica: indicazioni contraddittorie della Cassazione*" in Cassazione Penale, n. 1/2001

F. Antolisei, "*Manuale di diritto penale, Parte speciale, I*", Giuffré, Milano, 2002.
S. Battaglia, "*Criminalità informatica al tempo di internet: rapporti tra phishing e riciclaggio*", articolo 18/09/2013 reperibile su Altalex: http://www.altalex.com/documents/news/2014/03/28/criminalità-informatica-al-tempo-di-internet-rapporti-tra-phishing-e-riciclaggio

G. Balmaceda Hoyos, "*El delito de estafa informática en el derecho europeo continental*", in Revista de Derecho y Ciencias Penales N. 17, 2011, Universidad San Sebastián (Chile)

F. Berghella – R. Blaiotta, "*Diritto penale dell'informatica e beni giuridici*", in Cassazione penale, 1995.

F. Bricola, "*Legalità e crisi, l'articolo 25 c. 2 e c. 3 Cost., rivisitato alla fine degli anni '70*", in Quest. Crim. 1980, p. 193

A. Bondi, A. Di Martino, G. Fornasari, "*Reati contro la pubblica amministrazione*", Giappichelli, 2008.

R. Borruso, "*Gli aspetti legali nella sicurezza nell'uso delle carte di credito e di pagamento*", in Giust. Civ., 1992, II, 217.

R. Borruso, G. Buonuomo, G. Corasaniti, D'Aietti, "*Profili penali dell'informatica"*, Giuffrè, Milano, 1994.

F. Cajani, G. Costabile, G. Mazzaraco, "*Phishing e furto d'identità digitale – Indagini informatiche e sicurezza bancaria*", Giuffrè Editore, 2008.

F. Cajani, D. D'Agostino, W. Vannini, "*Di necessità, virtù: appunti per una strategia globale al contrasto del cybercrime. L'esperienza del pool dei reati informatici della Procura di Milano*", in "IISFA Memberbook 2011 DIGITAL FORENSICS, Condivisione della conoscenza tra i membri dell'IISFA ITALIAN CHAPTER", Experta, Forlì.

M. Casella, "*Il furto dell'identità personale nella sua più lata accezione: il fenomeno digitale del 'Phishing'*", articolo del 29/03/2015.

C. Castronovo, a cura di, "*Manuale di diritto privato europeo, Volume 2*", Giuffrè Editore, Milano, 2007.

J. Antonio Choclán Montalvo, "*Fraude informático y estafa por computación*", en "Internet y Derecho penal", Cuadernos de Derecho Judicial, (X-2001)

P. Cipolla, "*Social network, furto d'identità e reati contro il patrimonio*" in Giur. merito, 2012, 12.

R.V. Clarke, "*Situational Crime Prevention: Successful Case Studies*", 1997, 2nd Edition, Albany, NY: Harrow & Heston.

J. Córdoba Roda, M. García Arán, "*Comentarios al Código Penal, parte especial*", Aranzadi, 2004.

M. Cuniberti, G.B. Gallus, F.P. Micozzi, S. Aterno, "*Cybercrimine: prime note sulla legge di ratifica della Convenzione di Budapest*", articolo del 08/05/2008, aggiornato il 08/03/2014 reperibile su Altalex:

http://www.altalex.com/documents/news/2014/03/08/cybercrimine-prime-note-sulla-legge-di-ratifica-della-convenzione-di-budapest

L. Cuomo, R. Razzante, "*La disciplina dei reati informatici*", Giappichelli, Torino, 2007.

L. Cuomo, "*Reati informatici – Suprema Corte di Cassazione: la creazione di un profilo su social network utilizzando le altrui sembianze integra il reato di sostituzione di persona*", Quotidiano Giuridico IPSOA.

G. D'Aietti, in Borruso ed altri, "*Profili penali dell'informatica*", Giuffrè, Milano, 1994

V. S. Destito, G. Dezzani, C. Santoriello, "*Il diritto penale delle nuove tecnologie*", Padova, Cedam, 2007.

A. Diani, "*Phishing: responsabilità della banca o del cliente? I profili civilistici*", 6/12/2011, http://www.quagliarella.com/ceb14.html

D. D'Agostini, "*Diritto penale dell'Informatica – Dai Computer Crimes alla Digital Forensic*", Esperta, Forlì, 2007.

A. Del Ninno, "*Ricostruzione preliminare del quadro normativo in materia di identità digitale e furto di identità nell'ordinamento italiano*", 2015, su www.dirittoegiustizia.it/news

A. Di Tullio D'Elisiis, "*Frode informatica commessa con sostituzione d'identità digitale: profili applicativi*", articolo 14/01/2014, reperibile su Altalex: http://www.altalex.com/index.php?idnot=66034

G. Faggioli, "*Computer Crimes*", Simone, Napoli, 2002.

A. Fanelli, "*La truffa*", seconda ed., Giuffré editore, 2009.

G. Fiandaca – E. Musco, "*Diritto penale – Parte generale*", sesta ed., Zanichelli, 2009.

C. Flick, "*Falsa identità su internet e tutela penale della fede pubblica degli utenti e della persona*", in Riv. Inf. e informatica 2008, 4-5.

R. Flor, "*Phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente*", Riv. it. dir. e proc. pen., fasc. 2-3, 2007, p. 899.

D. Fondaroli, "*La tutela penale dei beni informatici*", in Diritto dell'informazione e dell'informatica, 1996.

S. Frattallone, "*Phishing, fenomenologia e profili penali: dalla nuova frode telematica al cyber riciclaggio*", in Global Trust, www.globaltrust.it/documents/press/phishing/

V. Frosini, "*Informatica, diritto e società*", Giuffré, Milano, 1992

J. García García-Cervigón, "*El fraude informático en España e Italia – Tratamiento jurídico-penal y criminológico*", in "Revista cuatrimestral de las Facultades de Derecho y Ciencias Economicas y Empresariales", n. 74, mayo-agosto 2008.

M. Giuseppe, "*La competenza territoriale in materia di reati informatici, fra giurisdizione di legittimità e profili di incostituzionalità: brevi note a margine della sent. Cass. Pen. n. 45078/2008*", 2009, in www.diritto.it

M. Gonzáles Suárez, "*Fraudes en Internet y Estafa Informatica*", Trabajo fin de Master, Universidad de Oviedo, Mayo 2014.

M. Grotto, "*Reati informatici e convenzione cyber crime. Oltre la truffa e la frode informatica: la frode del certificatore*", in Dir. inform., 2009.

S. Logroscino, "*La frode informatica quale autonoma figura di reato rispetto al delitto di truffa*", articolo del 21/12/2011, reperibile su Altalex: http://www.altalex.com/index.php?idnot=16607

L. Luparia, "*I correttivi alle distorsioni sistematiche*", in "*Le nuove norme sulla sicurezza pubblica*" di S. Lorusso, Cedam, 2008.

C. Maioli, E. Sanguedolce, "*I "nuovi" mezzi di ricerca della prova fra informatica forense e L. 48/2008*", articolo del 7/05/2012 reperibile su Altalex al seguente link: http://www.altalex.com/documents/altalex/news/2012/05/03/i-nuovi-mezzi-di-ricerca-della-prova-fra-informatica-forense-e-l-48-2008

A. Manna, "*Artifici e raggiri on-line: la truffa contrattuale, il falso informatico e l'abuso dei mezzi di pagamento elettronici*", in Diritto dell'informazione e dell'informatica, 2002, 995.

A. Masi, "*Frodi informatiche e attività bancaria*" in Rivista penale dell'economia, 1995, fasc. 4.

G. Malgieri, "*La nuova fattispecie di 'indebito utilizzo d'identità digitale – un problema applicativo*", 22/10/2014, reperibile su Altalex: http://www.penalecontemporaneo.it/upload/1413493350MALGIERI_2014.pdf

G. Malgieri, "*Il furto di 'identità digitale': una tutela 'patrimoniale' della*

personalità", in "*La giustizia penale nella rete. Le nuove sfide della società dell'informazione nell'epoca di Internet*", a cura di R. Flor, D. Falcinelli, S. Marcolini, ed. DiPLaP, 2014.

F. Mantovani, "*Diritto penale, Parte speciale, delitti contro il patrimonio*", Cedam, Padova, 2002.

G. Marini, "*Digesto delle opere penalistiche,* (voce) *Truffa (Frode informatica)",* Torino, 2006.

V. Militello, "*Nuove esigenze di tutela penale e trattamento elettronico delle informazioni*", in Rivista trimestrale di diritto penale dell'economia, 1992, p. 373-374.

V. S. Moccia, "*Tutela penale del patrimonio e principi costituzionali*", Cedam, Padova, 1998.

O. Morales García in "*Principios de derecho de la sociedad de la información*", Aranzadi, Thomson Reuters, 2010.

F. Mucciarelli, "*Commento dell'art. 10 della l. 23/12/1993, n. 547*", in Legislazione Penale, 1996.

R. S. Murphy, "*Property rights in personal information*", 1996, in http://www.lexisnexis.com/

C. Del Re, "*La frode informatica*", ed. Polistampa, 2009.

Intervento Onorevole S. Boccadutri tenutosi innanzi alla Camera dei Deputati, seduta n. 93 del 9/10/2013, in www.camera.it

Intervento Onorevole A. Gargano tenutosi innanzi alla Camera dei Deputati, seduta n. 93 del 9/10/2013, in www.camera.it

T. Padovani, "*Diritto Penale*", X ed., Milano, 2012.

A. Pagliaro, "*Principi di diritto penale, Parte speciale, Delitti contro il patrimonio*", Milano, 2003

A. Palmieri, nota a sentenza del Tribunale Milano, sez. VI civile, del 04/12/2014, 23/01/2015, reperibile su Altalex al seguente link: http://www.altalex.com/documents/news/2015/01/22/home-banking-risarcibili-i-danni-da-phishing

C. Parodi, "*La frode informatica: presente e futuro delle applicazioni criminali*

nell'uso del software, in Diritto penale processuale, 1997.

C. Parodi, "*La tutela penale dei sistemi informatici e telematici: le fattispecie penali*", Relazione presentata al Convegno Nazionale su "Informatica e riservatezza" del Centro Nazionale Universitario di Calcolo Elettronico, Pisa 26/27 settembre 1998

S. Piancastelli, "*La ricezione di somme di denaro provento di phishing: risultanze investigative e problemi applicativi in punto di qualificazione giuridica*", articolo del 3/03/2015 reperibile su Altalex: http://www.penalecontemporaneo.it/upload/1425310189PIANCASTELLI_2015a.pdf

G. Pica, "*Diritto penale delle tecnologie informatiche*", UTET, Torino, 1999.

L. Picotti, "*Il diritto penale dell'informatica nell'epoca di Internet*", Cedam, Padova, 2004.

L. Picotti, "*La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*", 2008.

C. Pecorella, "*Diritto penale dell'informatica*", II ed., Cedam, Padova, 2006.

F. Pesce, "*Alle radici di un difficile binomio: analisi economica e diritto penale*", in Indice penale, nuova serie, anno XIV, n. 1, Gennaio-Giugno 2011, CEDAM.
M. Romani, D. Liakopoulos, "*La globalizzazione telematica*", Giuffré, Milano, 2009.

C. Sarzana di S. Ippolito, "*Informatica, internet e diritto penale*", ed. rivista e aggiornata, Giuffré, Milano, 2010.

U. Sieber, "*La tutela penale dell'informazione*", in Rivista trimestrale di diritto penale dell'economia, 1992, p. 492.

G. Spangher, "*Trattato di procedura penale – 1. soggetti e atti*", UTET, 2009.

G. Stalla, "*L'accesso abusivo ad un sistema informatico o telematico*", reperibile su: www.penale.it/commenti/stalla01_html

Suárez Gonzáles, en R. Mourullo (dir.)/J. Barreiro (coord.), "*Comentarios al Código Penal*", Madrid: Editorial Civitas, 1997

A. Torrente, P. Schlesinger, in "*Manuale di diritto privato*", Giuffrè Editore, 2009.

L. Viola, "*Ingiusto profitto e danno altrui nella c.d. truffa contrattuale*", settembre

2003, su: http://www.diritto.it/articoli/penale/viola.html

F. Vitale, "*Brevi riflessioni sul reato di "frode informatica: i servizi a contenuto applicati dalle compagnie telefoniche nell'alveo dei cyber crime*", in Archivio penale, n. 1, www.archiviopenale.it.

D. Vulpiani, "*La nuova criminalità informatica. Evoluzione del fenomeno e strategie di contrasto*", in Rivista di Criminologia, Vittimologia e Sicurezza Vol. I, n. 1, Gennaio-Aprile 2007.

Giurisprudenza:

Cass. Pen., sez. II, sent. n. 7730 del 3/04/1986

Cass. Pen, sez. V, sent. n. 16304 del 27/11/1989 (ud. 20/09/1989)

Cass. Pen., sez. II, sent. n. 1162 del 7/12/1989, *Maiello*

Cass. Pen. sez. V, sent. n. 4295 del 24/4/1996

Cass. Pen., sez. II, sent. n. 2436 del 27/02/1997

Cass. Pen., sez. II, sent. n. 12027 del 23/12/1997, *Marrosu*

Cass. Sez. Unite, sent. del 16/12/1998

Cass. Pen., sez. VI, sent. n. 3065 del 14/12/1999 (ud. 04/10/1999), De Vecchis.

Cass. Pen., sez. VI, sent. n. 3067 del 14/12/1999 (ud. 04/10/1999), Piersanti.

Cass. Pen., sez. Unite, 28/03/2001, *Tiezzi*.

Cass. Pen., sez. V, sent. n. 23429 del 8/06/2001

Cass. Pen., sez. I, sent. n. 37115 del 2/10/2002

Cass. Pen., sez. V, sent. n. 24816 del 6/06/2003, *Ferruti*.

Cass. Pen., sez. I, sent. n. 26046 del 18/06/2003 (cc. 28/05/2003), Silletti.

Cass. Pen., sez. II, sent. n. 32440 del 31/07/2003 (ud. 10/07/2003), Larné.

Cass. Pen., sez. II, sent. n. 41451 del 23/09/2003

Cass. Pen., sez. V, sent. n. 44362 del 19/11/2003

Cass. Pen. sez. I, sent. n. 42888 del 26/10/2004

Cass. Pen., sez. III, sent. n. 5728 del 15/02/2005

Cass. Pen., sez. I, sent. n. 9395 del 9/03/2005

Cass. Pen., 18/05/2005, *Daiu*, in Cass. Pen. 2006

Cass. Pen., sez. V, sent. n. 6695 del 12/12/2005

Cass. Pen., sez. IV, sent. n. 17386 del 19/05/2006

Cass. Pen., sez. II, sent. n. 19831 del 9/06/2006, *Mohammad*

Cass. Pen., sez. II, sent. n. 31990 del 14/06/2006

Cass. Pen., Sez. V, sent. n. 46674 del 9/11/2007

Cass. Pen., sez. II, sent. n. 10085 del 05/03/2008

Cass. Pen., sez. II, sent. n. 27950 del 18/06/2008

Cass. Pen., sez. V, sent. n. 1727 del 30/09/2008 (ud. 30/09/2008), R.U.

Cass. Pen., sez. I, sent. n. 45078 del 30/10/2008 (dep. 4/12/2008), Gip Tribunale Napoli c. Gip Tribunale Nola.

Cass. Pen., sez. II, sent. n. 6783 del 17/02/2009

Cass. Pen., sez. VI, sent. n. 16669 del 11/03/2009 (ud. 11/03/2009) Pubblico Ministero presso Tribunale di Palermo c. S.C.

Cass. Pen., sez. II, sent. n. 40790 del 23/10/2009;

Cass. Pen., sez. II, sent. n. 44720 del 11/11/2009 (ud. 11/11/2009), G.G.

Cass., sez. Unite, sent. n. 12433 del 26/11/2009;

Cass. Pen., sez. V, sent. n. 27135 del 19/03/2010 (ud. 19/03/2010).

Cass. Pen., sez. II, sent. n. 6958 del 25/01/2011.

Cass. Pen., sez. II, sent. n. 9891 del 11/03/2011 (ud. 24/02/2011).

Cass. Pen., sez. II, sent. n. 17748 del 15/04/2011 (ud. 15/04/2011).

Cass. Pen., Sez. Fer., sent. n. 45946 del 15/09/2011 (dep. 12/12/2011)

Cass. Pen., sez. III, sent. n. 12479 del 15/12/2011 (dep. 3/04/2012)

Cass. Pen., sez. II, sent. n. 11699 del 10/01-28/03/2012

Cass. Pen., sez. III, sent. n. 23798 del 15/06/2012, Pres. De Maio, rel. Mulliri.

Cass. Pen., sez. V, sent. n. 18826 del 28/11/2012

Cass. Pen., sez. II, sent. n. 13475 del 06/03/2013 (dep. 22/03/2013).

Cass. Pen., sez. II, sent. n. 18909 del 30/04/2013 (ud. 10/04/2013).

Cass. Pen., sez. II, sent. n. 37170 del 11/09/2013.

Cass. Pen., sez. I, sent. n. 40303 del 27/05/2013 (dep. 27/09/2013).

Cass., sez. Unite, sent. n. 40354 del 18/07/2013

Cass. Pen., sez. III, sent. n. 52512 del 22/05/2014 (dep. 18/12/2014)

Cass. Pen., sez. V, sent. n. 25774 del 16/06/2014

Cass. Pen., sez. I, sent. n. 46101 del 07-10/07-11-2014

Cass. Pen., sez. V, sent. n. 25774 del 16/06/2014 (ud. 23/04/2014).

Tribunale di Milano, 8 novembre 2006, in *Giur. Merito*, 2012, 9, 1936

Tribunale di Milano, 10/12/2007 (sent.), G.I.P. Gamacchio.

Tribunale di Milano del 28/07/2006 in "Diritto di Internet", 2007

Giudice di Pace di Lecce, sent. n. 128/08

Giudice di Pace di Badolado, sent. n. 837/08

Trib. di Palermo, sez. II, sent. n. 2904 del 11/06/2011 - Giudice Dott.ssa Spiaggia

Tribunale di Milano, 7/10/2011 (sent.), Pres. Pellegrino, Est. Corbetta.

Tribunale Milano, uff. G.I.P., sent. n. 2507 del 10/04/2013, giud. Ferraro, imp. Ciavarella.

Tribunale di Milano, sez. VI penale, sent. n. 6753 del 28/05/2013, giud. Bernazzani, imp. Trozzola.

Tribunale di Napoli, G.U.P. Gallo, sent. n. 1653 del 4/07/2013

Trib. Milano, sez. VI penale in composizione monocratica – sent. 6753/2013 (est. Bernazzani)

Trib. di Firenze, sez. III civile, sent. del 20/05/2014

Trib. di Milano, sez. VI civile, sent. del 04/12/2014

Tribunal Supremo (STS) del 19 aprile 1991 (RJ 1991, 2813)

Tribunal Supremo (STS) sentencia del 20/11/2001 (RJ 2002, 805)

Tribunal Supremo (STS) sentencia de 12/06/2007 (RJ 2007, 3537);

Tribunal Supremo (STS) sentencia 8284/2012 de 25/10/2012. Sala de lo Penal. Sección Primera. N. de Recurso: 2422/2011. N. de Resolución: 834/2012. Ponente: Manuel Marchena Gómez

Tribunal Supremo (STS) sentencia de 12/06/2007, EDJ 2007/70163

<u>Relazioni</u>

Cassazione Relazione III/01/2013, "*Novità legislative: D.L. 14 agosto 2013, n. 93 "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", Roma, 22/08/2013.

Cassazione, Ufficio del massimario, Rel. N. 41/14, *Orientamento di giurisprudenza*, 2014

Dossier del Servizio studi sull'A.S. n. 1079 "*Conversione in legge, con modificazioni, del decreto-legge 14 agosto 2013, n. 93, la locuzione "furto o indebito utilizzo dell'identità digitale" in luogo della locuzione "sostituzione dell'identità digitale", impiegata dal decreto-legge*", edizione provvisoria, ottobre 2013, n. 64, pag. 103, in www.senato.it.

Relazione alla Camera dei Deputati di presentazione del Disegno di Legge n. 1540 di conversione del decreto-legge 14 agosto 2013, n. 93, presentato il 16/08/2013: http://www.camera.it/

Relazione della deputata A. D. Ferranti relatore per la II Commissione, anche a nome del deputato F. P. Sisto, relatore per la I Commissione, in sede di discussione sulle linee generali del disegno di conversione n. 1540-A, in www.camera.it

Procura della Corte di Cassazione, "*Principali orientamenti della Procura Generale sulla risoluzione dei contrasti*", a cura di Fulvio Baldi

Rapporto Clusit 2015

Relazione primo anno di attività di EC3 (2014)

Rapporto statistico 4/2014 UCAMP
(http://www.governo.it/backoffice/allegati/76514-9625.pdf)

Altre fonti

Comunicazione della Commissione Europea "*Verso una politica generale di lotta contro la cibercriminalità*" (COM (2007) 267)

OCSE, "*Scoping Paper on Online Identity Theft*", 18 giugno 2008, Section I.
Ricerca ISACA sulla sicurezza informatica commissionata da Trend Micro Inc. (http://www.trendmicro.it/newsroom/pr/la-nuova-ricerca-isaca-sulla-sicurezza-informatica-commissionata-da-trend-micro-rivela-che-unazienda-su-cinque-ha-subito-un-attacco-apt-/)

Manuale operativo di SCIPAFI (2015)

(http://www.dt.tesoro.it/export/sites/sitodt/modules/documenti_it/prevenzione_reati_finanziari/prevenzione_reati_finanziari/Manuale_operativo_15_gennaio_2015.pdf)

Sitografia

www.abilab.it

www.altalex.com

www.camera.it

www.senato.it

http://conventions.coe.int/Treaty/en/Treaties/PDF/Italian/185-Italian.pdf

www.cortedicassazione.it

www.diritto.it

www.governo.it

www.penalecontemporaneo.it

www.penale.it

www.procuracassazione.it

www.ricercagiuridica.com

www.studiocataldi.it

it.wikipedia.org/wiki/Identità_digitale

http://www.anti-phishing.it/

https://www.d3lab.net/index.php/blog/126-stat-1-sem-2013

https://www.sophos.com/it-it/press-office/press-releases/2006/04/pr_it_phishstats.aspx

Sans Institute System administration, networking*:* http://www.sans.org/

OLAF: http://ec.europa.eu/anti_fraud/index_en.htm

ENISA: https://www.enisa.europa.eu/

European Cybercrime Centre: https://www.europol.europa.eu/ec3

Cybercrime repository (UNODC): https://www.unodc.org/cld/index-cybrepo.jspx
https://www.commissariatodips.it/profilo/cnaipic.html

https://it.wikipedia.org/wiki/Centro_nazionale_anticrimine_informatico_per_la_protezione_delle_infrastrutture_critiche

http://www.interno.gov.it/it/temi/sicurezza/crimine-informatico/centro-nazionale-anticrimine-informatico-protezione-infrastrutture-critiche-cnaipic

http://www.abilab.it/web/sicurezza-e-frodi-informatiche

https://www.abi.it/Pagine/news/Intesa-tra-ABI-e-Polizia-.aspx

http://www.dt.mef.gov.it/it/antifrode_mezzi_pagamento/prevenzione_frodi_mezzi_pagamento/

https://sipaf.tesoro.it/SIPAF/faces/xhtml/protected/home.xhtml

http://www.consap.it/fondi-e-attivita/supporto/furto-d-identita

http://www.dt.tesoro.it/it/antifrode_mezzi_pagamento/furto_identita/sistema_prevenzione.html

http://www.dt.tesoro.it/it/antifrode_mezzi_pagamento/furto_identita/

http://www.boe.es/buscar/act.php?id=BOE-A-1995-25444

www.elderecho.com

http://porticolegal.expansion.com/pa_articulo.php?ref=407
https://herrerogimenezabogado.wordpress.com/2013/01/02/jurisprudencia-phishing-diferentes-figuras-delitivas-concurso-aparente-de-normas-penales/#_ftn1

http://portaley.com/

http://portaljuridico.lexnova.es/