FRANCESCO VITALE

Brevi riflessioni sul reato di "frode informatica": i servizi a contenuto applicati dalle compagnie telefoniche nell'alveo dei *cybercrime*

1. Nella nuova era digitale, i rapporti giuridici si snodano in modo a volte tortuoso, ma affascinante, sempre di più in campi fino a 20 anni fa inesplorati, o appena sfiorati. Le nuove tecnologie, le cui interfacce "portatili" sono rappresentate dagli schermi di *computer*, *tablet* e *smartphone*, assumono un ruolo di primo piano nelle relazioni umane e, di conseguenza, nel diritto: dai contratti a distanza, all'*e-commerce*, dalle procedure amministrative, ai *cybercrime*, il fulcro di molti rapporti umani si articola, su un piano paritario, tra "io fisico" e "io-*online*"[1].

Le ripercussioni di tale momento storico e antropologico, nonché, ovviamente, tecnologico, si sviluppano non soltanto su quelli che sono i rapporti leciti tra individui, ma anche e, ahimè, soprattutto su una vasta gamma di condotte illecite e criminali di non sempre facile analisi ed individuazione. Sul punto, le relazioni di molti magistrati durante l'inaugurazione dell'anno giudiziario 2015 presso i diversi distretti delle corti d'appello dislocate sul territorio italiano hanno rivelato alcuni dati interessanti: i crimini informatici sono in crescita del 400%[2].

In realtà, se è vero che senza dubbio più facile è difendersi da fenomeni criminali la cui origine si riconduce a condotte illecite promananti da singoli individui (ancorché insidiose) operanti in autonomia e col fine, solitamente, di conseguire un profitto personale, cosa ben diversa è rappresentata da quelle condotte criminose in cui soggetto autore della condotta delittuosa sia una grande società, peraltro posta sul piano di "parte forte" nell'ambito di un rapporto contrattuale con i privati.

Tali condotte, ancor più pericolose e ingannevoli perché provenienti da sog-

---

[1] Credo che in argomento illuminante sia il saggio di RODOTÀ, *Il mondo della rete. Quali i diritti, quali i vincoli,* Roma, 2014.

[2] Con espresso riferimento ai reati informatici, si veda, tra gli altri, D'AIUTO, LEVITA, *I reati informatici. Disciplina sostanziale e questioni processuali*, Milano, 2012; CUOMO, RAZZANTE, *La nuova disciplina dei reati informatici*, Torino, 2009; FAGGIOLI, *Computer crimes*, Napoli, 2002; ALMA, PERRONI, *Riflessioni sull'attuazione delle norme a tutela dei sistemi informatici,* in *Dir. e proc. pen.*, 1997, 506; GALDIERI, *Teoria e pratica nell'interpretazione del reato informatico*, Milano, 1997; CECCACCI, *Computer crimes,* Milano, 1994; FROSINI, *Introduzione*, in BORRUSO, BUONOMO, CORASANITI, D'AIETTI, *Profili penali dell'informatica*, Milano, 1994, XIII; GIANNANTONIO, *I reati informatici*, in *Il diritto dell'informazione e dell'informatica*, 1992, 336.

getti qualificati, pongono l'interrogativo di non poco conto sulla necessità e, anzi, opportunità di apprestare un'effettiva tutela penale, parallelamente alle tutele di natura civile e amministrativa già previste dall'ordinamento. La definizione di tale problematica solleva intricati interrogativi, anche e alla luce delle innumerevoli disquisizioni della dottrina penalistica in merito al cosiddetto "panpenalismo" e alla necessità di assoggettare al diritto dei reati molte delle situazioni giuridiche già regolate dal diritto civile e amministrativo[3].
In realtà, nonostante il diffuso pregiudizio di considerare la branca del diritto dei consumatori come incorporata strettamente all'area del diritto civile, in una società moderna tutte le disposizioni che tutelano il consumatore sono caratterizzate da una vera e propria "trasversalità": il consumatore deve quindi essere considerato meritevole di tutela in tutti i settori giuridici in cui si ritrova a ricoprire tale veste, dunque anche una tutela penalistica quando i suoi diritti e interessi siano posti in pericolo o lesi da condotte caratterizzate da un alto grado di offensività criminosa.
Con riferimento a tali questioni, si rivela di estrema attualità la problematica relativa al caso dei "servizi a contenuto" o "servizi *premium*" non richiesti dal consumatore e applicati dalle compagnie telefoniche ai titolari di utenze mo-

[3] Sul problema, tra i più estesi e controversi nell'analisi del diritto penale alla luce delle altre branche dell'ordinamento, ed in particolare sul rapporto di equilibrio tra sanzione penale e sanzione extrapenale, innumerevoli contributi si registrano in dottrina. Per un collegamento tra teoria del bene giuridico, principio di proporzionalità e principio di stretta necessità dell'intervento penale si veda DE FRANCESCO, *Diritto penale. I fondamenti*, Torino 2008, 11. Già in tempi non sospetti, in un panorama di parte speciale in molte parti diverso dal presente, PALAZZO, *Il principio di determinatezza nel diritto penale,* Milano 1979, 104, ha parlato di un vero e proprio «scadimento del Parlamento quale tutore della legalità, nella crescente produzione legislativa di leggi vuote (simboliche), compromissorie, o semplicemente sciatte»; DOLCINI, *Sanzione penale o sanzione amministrativa: problemi di scienza della legislazione,* in MARINUCCI, DOLCINI, *Diritto penale in trasformazione*, Milano 1985, 371. Ulteriori importanti contributi al dibattito su panpenalismo e diritto penale come *extrema ratio,* ROMANO, *Danno a sé stessi, paternalismo legale e limiti del diritto penale,* in *Riv. it. dir. proc. pen.*, 2008, 993; EUSEBI, *Ripensare le modalità della risposta ai reati traendo spunto* da Corte eur. dir. uomo, 19 giugno 2009, Sulejmanovic c. Italie, nota a Corte eur. dir. uomo, 16 luglio 2009, Sez. II, in *Cass. pen.*, 2009, 4952. L'autore ha proposto di recuperare il sistema delle sanzioni penali alla progettazione politico-criminale, sottolineando come la scelta di qualsivoglia opzione applicativa non potrà mai avere alcun rigore matematico, né, eventualmente, essere considerata logica se non alla stregua di criteri che non sono esclusivo appannaggio della materia penalistica, ma che abbraccino molteplici settori dell'ordinamento: tale riflessione evidenzia il punto di fatto di maggior problematica nell'ultimo trentennio di legislazione penalistica, ossia l'introduzione di determinate norme incriminatrici sulla base della mera "aspettativa popolare", finalizzate all'ottenimento del consenso, per l'autorevolezza che esse sono in grado di guadagnarsi nel contesto sociale, e non per la loro effettività e utilità; MUSCO, *L'illusione penalistica*, Milano 2004, 3; DONINI, *Il volto attuale dell'illecito penale. La democrazia penale tra differenziazione e sussidiarietà*, Milano 2004, 85. Con riferimento ai più recenti interventi legislativi si vedano i preziosi contributi di EUSEBI, *La riforma ineludibile del sistema sanzionatorio penale*, in *Riv. it. dir. proc. pen.*, 2013, 1307; PADOVANI, Alla ricerca di una razionalità penale, in *Riv. it. dir. proc. pen.*, 2013, 1087.

bili: nello specifico, migliaia di utenti, navigando coi propri *smartphone* su internet, o utilizzando applicazioni per cellulari e *tablet* si ritrovavano improvvisamente e senza saperlo abbonati a servizi *premium* per ricevere contenuti di mobilità, mai richiesti dal consumatore. L'Autorità Garante per la Concorrenza e il Mercato, a seguito di innumerevoli denunce dei consumatori, ha condotto un'indagine dalla quale sono risultati tali dati: su vari siti *web* e *app* si trovano *banner* pubblicitari (vere e proprie "strisce" sulle pagine internet la cui funzione è quella di *link* ad altri siti *web* riportanti offerte commerciali ecc.) apparentemente innocui, ma se l'utente vi effettua il *click* sopra, se pur inconsapevolmente, viene abbonato ai servizi offerti, i cui costi vengono automaticamente addebitati dall'operatore (TIM, Vodafone, ecc.) sul conto telefonico, scalando dal credito mobile determinati importi, più o meno consistenti. In alcuni casi, i *banner* sono anche invisibili, perché criptati all'interno del codice della pagina *web*, cosicché, aprendo la pagina, l'utente, senza esserne cosciente, vi clicca sopra con tutte le conseguenze sopra riportate[4].
L'Antitrust, in proposito, è stata chiara nell'affermare la corresponsabilità della condotta fraudolenta sia dei fornitori dei servizi a contenuto o delle pubblicità, sia degli operatori telefonici stessi, posta in essere a mezzo di una pratica commerciale scorretta concretantesi da un lato nell'omissione di informazioni sul fatto che il contratto di telefonia mobile sottoscritto pre–abilita le schede sim alla ricezione dei servizi a sovrapprezzo, nonché l'esistenza del blocco selettivo per impedire la loro ricezione e la necessità per l'utente che voglia utilizzarlo di doversi attivare mediante una richiesta esplicita di adesione alla procedura di blocco; dall'altro, attraverso l'adozione da parte dell'operatore di telefonia mobile di un comportamento qualificato come aggressivo, consistente nell'attuazione di una procedura automatica di attivazione del servizio e di fatturazione in assenza di qualsiasi autorizzazione da parte del cliente al pagamento, nonché di qualsiasi controllo sulla attendibilità delle richieste di attivazione provenienti da soggetti quali i fornitori di servizi estranei al rapporto negoziale fra utente e operatore[5].

---

[4] Va segnalato, ad onor del vero, che ben 4 anni prima della decisione dell'Antitrust, con la quale è stato posto "nero su bianco" il problema, già la Procura della Repubblica di Milano, in Procedure Investigative, Sui primi accertamenti di polizia giudiziaria in materia di reati informatici, estratto da *Direttive per la polizia giudiziaria sui primi accertamenti investigati i in materia di reati informatici e modalità di trasmissione delle relative comunicazioni di notizia di reato alla procura di Milano*, Milano, 5 maggio 2011, 5, "bypassava" il problema del dibattito sull'applicazione o meno della sanzione penale al caso specifico: si disponeva in modo emblematico, infatti, che parallelamente alla procedura di conciliazione istaurata di fronte al Co.Re.Com., si potesse sottomettere querela all'Autorità giudiziaria in ordine al reato di frode informatica *ex* art. 640-*ter* c.p.

[5] Si fa espresso riferimento alla recente decisione AGCM, adunanza 13 gennaio 2015, caso Telecom-

Da tale pronuncia, si ricava chiaramente un dato: fino alla decisione dell'Antitrust, l'utente cliccava anche senza saperlo su programmi di collegamento criptati finalizzati all'applicazione "silenziosa" di tali servizi; l'operatore automaticamente passava all'addebito; l'operatore si spartiva i proventi con i fornitori dei servizi, ricavandone uno specifico vantaggio economico dall'elevata percentuale della "quota di spartizione", dimostrandosi ampiamente consapevole del meccanismo qui analizzato; solo nel caso in cui il consumatore si fosse accorto dell'"inganno", con una procedura *ex post* poteva bloccare la continuazione del servizio.
Tale meccanismo di attivazione dei servizi reso possibile dall'automatismo che caratterizza il sistema di trasferimento al *Content Service Provider* (CSP, fornitore di contenuti e servizi video–televisivi internet) dei codici di identificazione del cliente con la relativa fatturazione sul credito telefonico, rappresenta la causa cui ricondurre gli effetti segnalati dai consumatori consistenti in attivazioni non consapevoli e accidentali durante la navigazione *wap.* Il consumatore, anche a causa del solo sfioramento involontario del tasto di attivazione nella *landing page* (fenomeno tipicamente connesso ai comandi in *touchscreen* che caratterizzano gli *smartphone* utilizzati per l'attivazione) era ignaro di attivare un servizio a pagamento con addebito automatico sul suo credito/conto telefonico.

2. La concreta fattispecie in esame, sotto il profilo della tutela penale del consumatore, o più in generale, del privato cittadino nei rapporti contrattuali, ricalca la condotta criminosa tipica punita dall'art. 640-*ter* c.p., in tema di frode informatica, delitto introdotto nel 1993 dalla legge sui c.d. reati informatici per punire le truffe commesse, senza l'induzione in errore di una persona, ma, attraverso la manipolazione di un sistema informatico: esso, dunque, è posto a salvaguardia del patrimonio nella parte in cui ricomprende tutti quei mezzi e quegli strumenti finanziari che possono essere gestiti anche attraverso l'interfaccia di un computer o internet[6].

Wind-Vodafone-H3G, servizi *premium.*

[6] Già nel 2003, la Suprema Corte contribuiva alla definizione del reato in oggetto, affermando che «il reato di frode informatica (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 la manipolazione di detto sistema. Anche la frode informatica si consuma nel momento in cui l'agente consegue l'ingiusto profitto con correlativo danno patrimoniale altrui». Si veda, per l'appunto, Cass., Sez. V, 24 novembre 2003, Noto, in *Mass. Uff.,* n. 227459. Nella specie l'agente, utilizzando il sistema telefonico fisso installato in una filiale della Società italiana per l'esercizio telefonico, con la veloce e ininterrotta digitazione di numeri telefonici, in parte corrisponden-

La fattispecie incriminatrice della frode informatica punisce, con la reclusione, chiunque, alterando o intervenendo su un sistema informatico o telematico, o anche su dati, informazioni o programmi da questi utilizzati, consegue un ingiusto profitto, con altrui danno. Tale fattispecie è un tipico reato di evento a dolo generico, ed è perseguibile a querela nel caso in cui non ricorra alcuna circostanza aggravante.

In particolare, se si è già detto circa la finalità di tale presidio penale, ossia la tutela del patrimonio, esso in questo caso va inteso come l'insieme delle disponibilità finanziarie "immateriali" (si pensi, ad esempio, ai soldi e ai titoli depositati su di un conto corrente di una banca, la quale li gestisce attraverso un sistema informatico, o, con riferimento al caso di specie, il credito telefonico proprio di una privata utenza telefonica mobile) di cui si può disporre anche attraverso un computer[7].

Come di tutta evidenza, peraltro, il reato in esame è caratterizzato da uno schema fattuale analogo a quello della fattispecie di truffa di cui all'art. 640 c.p.[8].

---

ti a quelli per i quali il centralino era abilitato e in parte corrispondenti a utenze estere, era riuscito ad ottenere collegamenti internazionali, eludendo il blocco predisposto per le chiamate internazionali per le quali il sistema non era abilitato, così esponendo debitoriamente la Società italiana per l'esercizio telefonico nei confronti dei corrispondenti organismi esteri autorizzati all'esercizio telefonico. Sulle pronunce concernenti il rapporto tra frode informatica ed accesso abusivo a sistema informatica, si abbia riguardo a Cass., Sez. V, 19 dicembre 2003, P.m. in c. Comità, in *Riv. pen.*, 2005, 247. Con espresso riferimento al reato di frode informatica, ed al suo rapporto con altri reati informatici, poi, si vedano i numerosi contributi della dottrina, tra i quali, BARTOLI, *La frode informatica tra "modellistica", diritto vigente, diritto vivente e prospettive di riforma,* in *Dir. inf.*, 2011, 3, 383; PECORELLA, *Commento Art. 640-ter c.p.*, in *Codice penale commentato, Artt. 575-734-bis*, a cura di Marinucci, Dolcini, Milano, 2011, 6417; CAJANI, *Profili penali del phishing*, in *Cass. pen.*, 2007, 2294; FLOR, *Phishing, Identity Theft e Identity Abuse. Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. proc. pen.*, 2007, 899; RESTA, *Banche di dati on-line. I limiti della tutela penale*, in *Giur. mer.*, 2007, 2052; SCOPINARO, *Furto di dati e frode informatica*, in *Dir. pen. e proc.*, 2007, 364; ID., *Internet e reati contro il patrimonio*, 2007; PECORELLA, *Il diritto penale dell'informatica*, Padova, 2006; PICA, *Internet*, in *Dig. Pen.*, Torino, 2004, 425; PARODI, *Profili di rilevanza penale dei dialer*, in *Dir. pen. e proc.*, 2003, 1426; GUERNELLI, Frodi *informatiche e responsabilità delle persone giuridiche alla luce del d.lgs. 8 giugno 2001, n. 231*, in *Riv. trim. dir. pen. econ.*, 2002, 292; PARODI, *Commercio elettronico e tutela penale dei mezzi di pagamento*, in *Dir. pen. e proc.* 2001, 103; CERQUA, *Accesso abusivo e frode informatica: l'orientamento della Cassazione,* in *Dir. prat. soc.*, 2000, 51; CORRIAS LUCENTE, *Brevi note in tema di accesso abusivo e frode informatica: uno strumento per la tutela penale dei servizi,* in *Dir. inf.*, 2001, 492; PICA, *Reati informatici e telematici*, in *Dig. Pen.*, Aggiornamento, Torino, 2000, 521; PICOTTI, *Reati Informatici*, in *Enc. Giur. Treccani*, Roma, 1999; PARODI, *La frode informatica: presente e futuro delle applicazioni criminali nell'uso del software*, in *Criminalità informatica*, a cura di SARZANA DI S. IPPOLITO, in *Diritto e proc. pen*, 1997, 12, 1539.

[7] MANTOVANI, *Diritto penale, parte speciale*, II, *Delitti contro il patrimonio*, Padova, 2009, 210.

[8] Contro tale impostazione, se pur in modo pressoché isolato, si registra la tesi di PECORELLA, *Il diritto penale dell'informatica*, rist. con aggiornamento, Padova, 2006, 63. Più propriamente va detto che la norma fu introdotta dato che la truffa, essendo stata costruita sull'induzione in errore di del soggetto

Le condotte incriminate dall'art. 640-*ter* sono due: una consistente nell'alterazione in qualsiasi modo del funzionamento di un sistema informatico e telematico; l'altra nell'intervento senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti[9]. Tali condotte, però, assumono rilevanza penale soltanto se consentono di conseguire un ingiusto profitto con altrui danno, similmente a quanto previsto in ordine al reato di truffa.
L'elaborazione dei dati può essere effettuata sia da un singolo computer che da più computer tra loro connessi, ad esempio a mezzo di internet: a tal riguardo si parla di "sistema informatico semplice" e di "sistema informatico complesso"; un sistema telematico svolge, invece, una duplice funzione, perché la sua attività consiste nell'elaborare e/o trasmettere informazioni e dati già elaborati o da elaborare[10].

---

passivo del reato tramite raggiri ed artifici, era ritenuta dal Legislatore dell'epoca (giustamente) inadatta a punire le frodi commesse attraverso una manipolazione dei sistemi e dei dati informatici. Sul punto si veda l'orientamento di Cass., Sez. II, 24 febbraio 2011, D.L.P.M.C., in *Mass. Uff.*, n. 249675. In merito, anche l'autorevole ricostruzione di MUCCIARELLI, *Commento all'art. 10 della l. n. 547 del 1993*, in *Legisl. pen.*, 1996, 136. Altra parte della dottrina ha sostenuto che dal momento che l'art 640-*ter* è un reato informatico non si può non rilevare che questa stessa norma può anche essere considerata come volta a tutelare, sia pure soltanto indirettamente, il «regolare funzionamento dei sistemi informatici e telematici», nonché «la riservatezza che deve accompagnarne l'impiego». Tale impostazione è rinvenibile in ANTOLISEI, *Manuale di diritto penale, parte speciale*, Milano, 2008, 386. Ulteriori spunti sulla natura di tutela apprestata dalla norma in esame si ritrovano in PICA, *Internet*, in *Dig. Pen.*, Aggiornamento, I, Torino, 2007, 433, secondo il quale «non si può non riconoscere che il primo obiettivo perseguito dall'art. 640-*ter* non può che essere quello di punire quei "comportamenti comunicativi" che cagionano un danno patrimoniale ed economico, anche attraverso il solo spostamento di informazioni o dati».

[9] PECORELLA, *Commento Art. 640-ter c.p.,* in *Codice penale commentato, Artt. 575-734 bis*, a cura di DOLCINI, MARINUCCI, Milano, 2011, 6417. Nel caso della alterazione di un sistema non è rilevante se chi agisce è legittimato, o meno a farlo; mentre, in quello dell'intervento sui dati il disvalore della condotta si incentra proprio sulla circostanza che colui che ha agito lo ha fatto «senza diritto» (*contra*, PICA, *Diritto penale delle tecnologie informatiche*, Torino, 1999, 144, il quale ritiene che la seconda condotta costituisca una particolare ipotesi della prima). In ordine, poi, al concetto di sistema informatico e telematico, la Cassazione ha dato una univoca definizione «per sistema informatico o telematico deve intendersi un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate – per mezzo di un'attività di "codificazione" e "decodificazione" – dalla "registrazione" o "memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "dati", cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (*bit*), in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare "informazioni", costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente». Si vedano sul punto Cass., Sez. II, 15 aprile 2011, F.M.I. N., in *DeJure*; Id., Sez. II, 24 febbraio 2011, D.L.P.M.C., in *Mass. Uff.,* n. 249675; Id., Sez. VI, 04 ottobre 1999, Piersanti, in *Cass. pen.*, 2000, 2990, con note di ATERNO e CUOMO.

[10] Interessante notare già alcune pronunce della fine degli anni novanta sembrano aver voluto anticipare l'analisi del rapporto tra sistema informatico-telematico e gli strumenti di telefonia. Infatti, in Cass., Sez.

Chiaramente, la definizione di "computer" va aggiornata ed attualizzata, alla luce del fatto che un elaboratore elettronico di dati deve essere considerato qualsiasi *smartphone*: le funzionalità dei moderni cellulari, infatti sono ormai assimilabili in tutto a quelle di qualsiasi PC. Sotto tale profilo, quindi, si riscontra un primo elemento di assimilabilità tra la fattispecie concreta e la norma incriminatrice.
La condotta delle compagnie telefoniche, inoltre, così configurata rischia di configurarsi doppiamente fraudolenta, dato che le stesse, nell'ambito dell'"artificio tecnologico" inferto ai consumatori, si sono altresì avvalse, come ben specificato dalla decisione dell'Antitrust, dell'omissione di informazioni contrattuali che (violando in modo evidente il Codice del Consumo), se fornite, avrebbero evitato un danno patrimoniale ai contraenti[11].

3. Va detto che l'alterazione di un sistema informatico o telematico si configurerà tutte le volte in cui vi sia verificata una manipolazione, che abbia modificato, fraudolentemente, il regolare modo di operare del sistema[12]. Soprattutto

---

VI, 04 ottobre 1999, De Vecchis, in *Foro it.*, 2000, II, 133, si sottolineava che 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 all'uomo attraverso l'utilizzazione (anche in parte) di tecnologie informatiche, deve ritenersi che sia la rete telefonica di cui si serve la Telecom, sia il centralino di una singola filiale costituiscono un sistema che si avvale di tecnologie informatiche.

[11] E sul punto è d'obbligo sottolineare, senza voler scadere in eccessi sanzionatori e ispirazioni "inquisitorie", che facilmente si rischierebbe di incorrere in un eventuale concorso di reati con la fattispecie di truffa contrattuale. Come da ormai consolidata giurisprudenza, tale modalità di compimento dell'art. 640 c.p. si tipizza, sempre più spesso, con l'omissione di informazioni fondamentali nei confronti dell'altra parte contraente, quando quest'ultima è da considerare, se non un *minus habens*, quanto meno "svantaggiata": in questo caso, chiaro riferimento si fa al consumatore. Ancora una volta si rinvia a quanto affermato dall'AGCM, la quale ha spiegato che, in ogni caso, «la procedura prevista per l'attivazione dell'abbonamento essendo affidata ad un unico e semplice click, senza ulteriori passaggi, non consente al consumatore di poter acquisire piena consapevolezza del fatto che sta sottoscrivendo un servizio in abbonamento, immediatamente addebitato sul proprio credito telefonico, attraverso la cessione del proprio numero di telefono dall'operatore al soggetto che eroga il servizio (CSP)».

[12] Si rinvia nuovamente a PECORELLA, *Commento Art. 640-ter c.p.,* cit., 6417. Ancora di interesse si rivela, inoltre, Cass., Sez. II, 24 febbraio 2011, D.L.P.M.C., in *Mass. Uff.*, n. 249675. Con l'occasione la Corte ha ulteriormente ribadito il discrimine tra le due diverse modalità di condotta del reato, specificando che «per alterazione deve intendersi 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*. In altri termini, il sistema continua a funzionare ma, appunto, in modo alterato rispetto a quello programmato: il che consente di differenziare la frode informatica dai delitti di danneggiamento informatico (artt. 635-*bis, ter, quater, quinquies* c.p.) non solo perché in quest'ultimi è assente ogni riferimento all'ingiusto profitto ma anche perché l'elemento materiale dei suddetti reati è costituito dal mero danneggiamento dei sistemi informatici o telematici e, quindi, da una condotta finalizzata ad impedire che il sistema funzioni o perché il medesimo è reso inservibile (attraverso la distruzione o danneggiamento) o perché se ne ostacola gravemente il funzionamento (sul punto, in particolare, l'art. 635-*quater* c.p.). La seconda condotta prevista dall'art. 640-

con riferimento al caso qui analizzato, avente ad oggetto il fraudolento "attacco" al credito delle utenze telefoniche mobili dei servizi non richiesti, va detto che le alterazioni dei sistemi informatici o telematici consistono, per lo più, in delle vere e proprie manipolazioni dei programmi, ovverosia dei *software*, che i computer (e quindi, secondo quanto sopra specificato, anche gli strumenti moderni di telefonia mobile) 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[13].

Una volta appurate le condotte su descritte, è necessario verificare che le in-

ter c.p. è costituita dall'intervento "senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico (...)": si tratta di un reato a forma libera che, finalizzato pur sempre all'ottenimento di un ingiusto profitto con altrui danno, si concretizza in una illecita condotta intensiva ma non alterativa del sistema informatico o telematico». La decisione confermava la configurabilità del reato di cui all'art. 640-*ter* c.p., in quanto la condotta contestata era sussumibile nell'ipotesi «dell'intervento senza diritto su informazioni contenute in un sistema informatico» di cui alla seconda parte dell'art. 640-*ter*, co. 1, c.p. Infatti, anche l'abusivo utilizzo di codici informatici di terzi ("intervento senza diritto") – comunque ottenuti e dei quali si è entrati in possesso all'insaputa o contro la volontà del legittimo possessore ("con qualsiasi modalità") – è idoneo ad integrare la fattispecie di cui all'art. 640-*ter* c.p. ove quei codici siano utilizzati per intervenire senza diritto su dati, informazioni o programmi contenuti in un sistema informatico o telematico, al fine di procurare a sé o altri un ingiusto profitto. In una più recente pronuncia, Cass., Sez. II, 06 marzo 2013, S.G., in *Plurisonline,* gli Ermellini hanno ripreso l'analisi delle due condotte tipizzate nella fattispecie incriminatrice, affermando che per alterazione del «funzionamento di un sistema informatico o telematico» deve intendersi (*ex* art. 640-*ter* c.p.) 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*: si tratta di un reato a forma libera che, finalizzato pur sempre all'ottenimento di un ingiusto profitto con altrui danno, si concretizza in una illecita condotta intensiva ma non alterativa del sistema informatico o telematico (in altri termini, il sistema continua a funzionare ma, appunto, in modo alterato rispetto a quello programmato). In tale occasioni, la Corte ha ribadito la differenza tra le due modalità di attuazione del delitto, sottolineando come la seconda condotta, rappresentata dall'intervento senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un dato sistema informativo o telematico, pur finalizzata pur sempre all'ottenimento di un ingiusto profitto con altrui danno, «si concretizza in un'illecita condotta intensiva ma non alterativa del predetto sistema».

[13] La giurisprudenza della Suprema Corte, in Cass., Sez. V, 19 Marzo 2010, M.M. N., in *Riv. polizia*, 2011, 7, 469, si è così pronunciata sull'inserimento nelle cc.dd. *slot machine* di una seconda scheda, tale da modificarne fisicamente la modalità di funzionamento. Per la giurisprudenza, crediamo in modo corretto, integra il reato di frode informatica, previsto dall'art. 640-*ter* c.p., l'introduzione, in apparecchi elettronici per il gioco di intrattenimento senza vincite, di una seconda scheda, attivabile a distanza, che li abilita all'esercizio del gioco d'azzardo, trattandosi della attivazione di un diverso programma con alterazione del funzionamento di un sistema informatico. È chiaro come la pronuncia in esame abbia un'importante ripercussione sulla problematica qui in esame, concernente l'attivazione "silenziosa" dei cosiddetti "servizi a contenuto". Essa stessa, per sua natura, ed in base a quanto affermato dall'Antitrust presenterebbe in modo analogo quei caratteri di "attivazione di un diverso programma", tali da alterare il sistema informatico, tali, quindi, da configurare la condotta criminosa.

terferenze sui dati, sulle informazioni ed i programmi, o la modifica del contenuto o anche della funzione delle diverse componenti di un sistema informatico o telematico siano state poste in essere "senza diritto". Un simile intervento si classificherebbe tale, però, non solo nel caso in cui dovesse considerarsi illecito, senza alcun diritto, ma anche nel caso in cui il soggetto agente usi impropriamente, "male", o abusi di un diritto di cui è titolare: è evidente che l'illiceità dell'intervento rappresenta un elemento di tipicità del fatto, mancando il quale il fatto non può non considerarsi atipico. Nella frode informatica, infatti, l'agire "senza diritto" è un elemento del fatto tipico, perciò colui che agisce nell'esercizio di un diritto, correttamente esercitato, pone in essere un fatto che è diverso da quello descritto dalla fattispecie astratta[14]. Le manipolazioni dei dati da parte dell'*extraneus* rilevano, per altro, sia che riguardino i dati, le informazioni ed i programmi contenuti in un sistema informatico o telematico, sia che riguardino i dati le informazioni e i programmi "pertinenti" ad un siffatto sistema: e, pertinenti devono considerarsi tutti quei dati che pur essendo contenuti in supporti materiali "esterni" (come, ad esempio, memorie portatili) sono *input*, e cioè dati e informazioni che devono essere immessi nel sistema perché questo li possa elaborare, o *output*, che sono i dati che il computer ha già elaborato e, quindi, i risultati dell'elaborazione[15].
Come a breve si vedrà, anche sotto tale profilo si rivelano indicazioni molto precise sulla possibilità, nel caso di specie, di incardinare una responsabilità penale degli operatori di telefonia mobile, dato che pur avendo il diritto di gestire il sistema di accredito/addebito dei conti delle utenze mobili, tramite l'abuso di tale diritto, e quindi tramite il suo rispettivo cattivo utilizzo, sono intervenuti sul sistema informatico, manipolandone il funzionamento.

4. La frode informatica è un tipico reato di evento, perché le due condotte previste sono tipiche solo nel caso in cui presentino un nesso eziologico che le colleghi all'evento, che la norma individua espressamente nel conseguimento di un profitto ingiusto per sé o per altri: questo, a sua volta, deve essere suddiviso in due distinti accadimenti, perché deve essere stato causato dal «risultato irregolare del processo di elaborazione»[16].

---

[14] L'agire nell'esercizio di un diritto, correttamente esercitato, quindi, non scrimina, perché fa venire meno, a monte, la tipicità (*contra* MANTOVANI, op. cit., 201; nonché PICA, op. ult. cit., 146).
[15] PECORELLA, *Commento Art. 640-ter c.p.*, cit., 6418.
[16] Su tale passo sono altamente indicative le indicazioni dell'Autorità Garante. Nella decisione in oggetto, infatti, è stato statuito che «l'operatore di telefonia trae uno specifico vantaggio economico dalla commercializzazione dei servizi premium. Dalle evidenze istruttorie emerge, infatti, che Telecom non è

Sulla ingiustizia del profitto, pur riprendendosi la stessa nozione valevole in merito al reato di truffa, va sottolineato che nella frode informatica l'evento acquisisce rilevanza: l'ingiusto profitto, infatti, genera il danno patrimoniale sulla sfera giuridica del soggetto passivo del reato, tale da far assumere al danno il carattere di un vero e proprio "secondo evento". Se ne deduce che, considerando tale reato come posto a presidio del patrimonio e del regolare funzionamento dei sistemi informatici, il danno patrimoniale subito dal soggetto passivo del reato è il *quid pluris* che differenzia la frode dagli altri reati informatici, il cui danno si potrebbe anche dire è in *re ipsa.*

5. Come si diceva, il reato *de quo* è sanzionato a titolo di dolo generico. Il soggetto attivo, quindi, deve rappresentarsi e volere che attraverso l'alterazione del sistema informatico, o alternativamente attraverso la manipolazione dei dati riesce a conseguire un profitto ingiusto, con altrui danno. In effetti, il fatto che, come ha sottolineato l'Antitrust, le compagnie telefoniche, utilizzando lo "stratagemma" dei servizi a contenuto, abbiano gestito un traffico da un miliardo di euro è, di per sé, già indicativo in tal senso[17].
Ulteriori spunti di riflessione, con connotazioni decisamente applicative in merito alla questione *de facto,* si ricavano dal fatto che, in modo più che corretto, il Legislatore ha previsto l'applicazione della circostanza aggravante dell'essere stata la frode commessa con «abuso delle qualità di operatore del sistema»: per tale deve intendersi il c.d. *system administrator*, e cioè colui il quale, avendo la possibilità di accedere a tutte le parti del sistema, ha, *de facto*, il controllo pieno di tutte le diverse fasi del processo di elaborazione dati e

---

remunerata forfetariamente per i servizi forniti ai CSP (*Content Service Provider*), ma percepisce una elevata percentuale in media circa il (30-60%) di ciò che si ricava dai servizi erogati (meccanismo di *revenue sharing*)».

[17] Con riferimento il Garante ha aggiunto anche che «è l'operatore a rivelare al CSP, mediante il c.d. meccanismo di *enrichment*, l'identità del consumatore per effetto di un solo *click* su di una *landing page* non soggetta al suo controllo e, a seguito della conseguente richiesta proveniente dal CSP, a prelevare unilateralmente la somma corrispondente dal credito telefonico del cliente. A tale procedura peraltro, come di seguito illustrato, sono causalmente riconducibili alcuni dei fenomeni illustrati e, segnatamente, l'attivazione del servizio e il relativo addebito anche a seguito di un accesso accidentale da parte del consumatore ovvero in assenza di una espressa e consapevole manifestazione di volontà in tal senso», sottolineando come «non può infine trascurarsi che le risultanze istruttorie e, segnatamente, i reclami, evidenziano una ampia consapevolezza da parte di Telecom circa la sussistenza di attivazioni dei predetti servizi non richieste o comunque non consapevoli da parte dei propri clienti. Telecom deve, inoltre, considerarsi responsabile in qualità di coautore della diffusione, da parte di Acotel, di *landing page* che presentano omissioni informative rilevanti. Infatti, come contrattualmente previsto e dichiarato dalla stessa Telecom, le *landing page* (*click* sul pulsante che identifica il comando di chiusura del relativo *banner*) che consentono l'accesso ai servizi sono soggette alla supervisione dell'operatore e da quest'ultimo».

non chiunque sia abilitato ad operare alla *consolle* dell'elaboratore[18]. A tal proposito, come già accennato, non sembra potersi negare un'eventuale parallela responsabilità penale della compagnia telefonica: il sistema fraudolento implementato da parte dell'operatore di telefonia mobile è constato di un vero e proprio procedimento automatico di trasferimento del numero di telefono dell'utente ("*enrichment*") dal gestore telefonico ai CSP che editano i contenuti digitali a pagamento, e nel successivo automatico addebito del servizio sul credito telefonico dell'utente senza che quest'ultimo abbia mai adottato un comportamento attivo (inserimento del proprio numero telefonico o altro codice di riconoscimento). Proprio con riferimento a ciò può correttamente parlarsi di una vera e propria condotta consistita nella alterazione del sistema informatico di gestione del credito dei singoli utenti, da porsi in capo all'operatore telefonico.

Va da sé che sarebbe in ogni caso necessario individuare gli elementi utili in ordine all'istaurazione di un procedimento penale, se, come in base alle riflessioni appena compiute, le condotte degli operatori telefonici si considerassero meritevoli di tutela penale nell'alveo dell'art. 640-*ter* c.p.

A tal proposito, la competenza per materia sarebbe del Tribunale in composizione monocratica, con udienza preliminare per le ipotesi aggravate.

Come per tutti i reati informatici, non è escluso l'insorgere di difficoltà circa l'individuazione dell'esatto luogo della consumazione ai fini di incardinare un processo penale. In realtà, la Cassazione ha precisato che tale indicazione vada desunta dal luogo in cui una delle due condotte criminose tipizzate dalla norma abbia avuto inizio[19].

---

[18] Sul punto si vedano in particolare i commenti forniti da PECORELLA, *Commento Art. 615-ter c.p.,* in *Comm. c.p.*, cit., 5988. È ancora utile richiamare la decisione dell'AGCM: l'oggetto della contestazione non è, dunque, così come eccepito dall'operatore e rilevato da AGCOM, rappresentato da una mera modalità tecnica di trasferimento dati, ma dall'adozione da parte dell'operatore di una procedura fondata su un meccanismo automatico di attivazione del servizio e di fatturazione basato sull'assenza di qualsiasi autorizzazione da parte del cliente al pagamento e, in ogni caso, di informazione al riguardo fornita all'utente, nonché sull'assenza di qualsiasi controllo da parte dell'operatore telefonico sull'azione manuale assertivamente posta in essere dall'utente e sulla attendibilità delle richieste provenienti da soggetti estranei al rapporto negoziale che lega utente e operatore, che procede all'addebito sul conto telefonico del cliente senza controllare che l'utente abbia effettivamente cliccato sulla *landing page* ufficiale. Nel campo della telefonia mobile, infatti, in virtù dell'esistenza di rapporti contrattuali basati su SIM ricaricabili, funzionanti con credito pre-pagato e comunque con piattaforma tecnologica controllata dal professionista, quest'ultimo si trova nella condizione di poter eseguire in modo unilaterale le attivazioni di servizi, potendo altresì procedere – nei confronti dei titolari di SIM pre-pagata – al prelievo coattivo dal credito telefonico dei consumatori.

[19] In proposito, si veda Cass., Sez. III, 24 maggio 2012, C.A. e F.C., in *Mass. Uff.*, n. 253633, in *Mass. Uff. Cassazione, 2012,* la quale ha stabilito che ai fini della determinazione della competenza territoriale, nel reato di frode informatica il *locus commissi delicti* va individuato nel luogo di esecuzione della

Per quanto riguarda il *tempus commissi delicti,* come si diceva, esso andrebbe inquadrato nel momento in cui l'agente consegue l'ingiusto profitto[20].

attività manipolatoria del sistema di elaborazione dei dati, che può coincidere con il conseguimento del profitto anche non economico. (Fattispecie nella quale il luogo di commissione del reato è stato individuato nella sede della società gestita dagli imputati, presso la quale si trovavano i server contenenti i dati oggetto di abusivo trattamento).

[20] ALESIANI, *Il momento consumativo del delitto di frode informatica: indicazioni contraddittorie della Cassazione*, in *Cass. pen.*, 2001, 485. Inoltre, ai fini di una più completa disamina della materia, Cass., Sez. VI, 04 ottobre 1999, n. 3065, De Vecchis, in *Giur. it.,* 2000, 1911, *Riv. pen.*, 2000, 226. Il reato di frode informatica, previsto dall'art. 640-*ter* c.p., si consuma – non diversamente dal comune reato di truffa – nel momento in cui l'agente consegue l'ingiusto profitto, con correlativo danno altrui. (Nella specie, in applicazione di tale principio, è stato ritenuto che, trattandosi di collegamenti telefonici con l'estero abusivamente realizzati da dipendenti della Telecom mediante l'uso improprio di un sistema predisposto per il solo soddisfacimento di esigenze di servizio, il profitto fosse stato conseguito in ciascuno dei momenti in cui detti collegamenti erano stati ottenuti, e che si fosse verificato anche il danno per la Telecom, consistente nell'esposizione debitoria di quest'ultima, a termini di contratto, nei confronti delle imprese che gestivano i servizi telefonici nei paesi cui le comunicazioni erano dirette).