Archivio Penale
settembre–dicembre 2013 fascicolo 3 anno LXV
ISBN 978-88-548-6177-0
DOI 10.4399/97888548617704
pag. 799–819

Profili penali delle truffe *on–line*[*]

Claudia Pecorella, Massimiliano Dova

1. Uno sguardo al fenomeno delle truffe *on–line* attraverso i dati del "*pool* reati informatici" della Procura di Milano. Le truffe *on–line* costituiscono la variante moderna delle più tradizionali truffe contrattuali: si realizzano infatti in occasione della compravendita di beni e servizi su una piattaforma informatica, nell'ambito del sempre più diffuso sistema del commercio elettronico. Come dimostra l'esperienza del Tribunale di Milano — del quale utilizzeremo a titolo esemplificativo i dati relativi alle denunce pervenute negli anni 2010 e 2011 — il fenomeno ha assunto un rilievo tutt'altro che marginale, ancorché in un medesimo arco temporale le denunce per fatti di questo tipo siano solo una minima parte di quelle riguardanti il reato di truffa: nell'anno 2010, solo il 5% (455 su 9.190) delle denunce per truffa iscritte a registro presso la Procura della Repubblica erano state realizzate *on–line*.

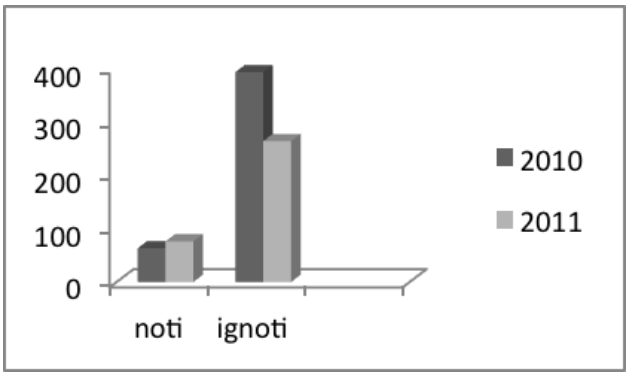
Nonostante il numero limitato delle denunce — che nel 2011 sono tra l'altro risultate in calo, essendone pervenute 339 — le truffe *on–line* sollevano complesse questioni che rendono difficoltose le indagini e poco probabile l'accertamento di una responsabilità penale, cosicché l'archiviazione è l'unica risposta possibile nella maggior parte dei casi. Uno sguardo ai dati presi a campione che, pur riferendosi a due anni diversi (ma consecutivi), mostrano una sostanziale omogeneità di risultati, consentirà di cogliere le caratteristiche di fondo del fenomeno e di comprendere gli aspetti più problematici della sua repressione penale.

Va detto innanzitutto che il numero delle notizie di reato con autore ignoto in questo settore è particolarmente elevato, tanto più se confrontato con quello delle truffe di tipo tradizionale: se per queste ultime la percentuale di denunce contro ignoti era nel 2010 intorno al 61%, quella relativa alle truffe su piattaforma informatica raggiungeva l'86% nello stesso anno (392 denunce su 455) e è di poco inferiore l'anno seguente (263 denunce su 339, equivalenti al 77,5% del totale).

L'analisi empirica fa emergere tuttavia un dato significativo: laddove vi è un indagato, si tratta spesso (nel 6% dei casi stando ai dati del 2011) di persona

[*] Il lavoro è frutto di riflessioni comuni agli autori. Sono tuttavia da attribuire a Claudia Pecorella i §§ 1–3 e a Massimiliano Dova i §§ 4–6.

con precedenti penali specifici o nei confronti della quale si sta procedendo per fatti analoghi. A ciò si aggiunga che, come talvolta emerge anche dalla ricostruzione dei fatti prospettata dal denunciante, nel caso (molto frequente) in cui si procede contro ignoti, il "nome utente" utilizzato per commettere la truffa è già noto in Rete, perché segnalato da altre vittime, con l'indicazione dei recapiti telefonici e dei dati bancari o postali, comunicati all'acquirente per ricevere il pagamento.

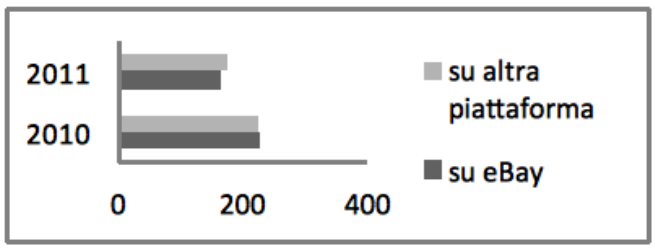


Luogo privilegiato di commissione del fatto risulta essere la piattaforma di *eBay*, tanto che tra gli addetti ai lavori è frequente l'impiego dell'espressione "truffe *eBay*" per indicare il fenomeno in esame: in danno degli utenti di questa piattaforma risultano realizzati ben 229 casi sui 455 (pari circa al 50%) nel 2010 e 163 su 339 nel 2011 (pari al 48%); i rimanenti casi vedono coinvolti utenti di diversi siti web di annunci gratuiti (come Secondamano.it, Subito.it, Bakeca.it, autoscout24.com) che, diversamente da *eBay,* agevolano la conoscenza delle richieste e delle offerte di beni e servizi ma non costituiscono il luogo virtuale nel quale concludere il contratto. La differenza tra questi due tipi di piattaforma risulta in realtà poco significativa ai nostri fini, perché dalla maggior parte delle denunce presentate alla Procura della Repubblica del Tribunale di Milano risulta che venditore e acquirente, pur essendosi 'incontrati' sulla piattaforma di *eBay*, hanno poi proseguito le trattative al di fuori di essa[1].

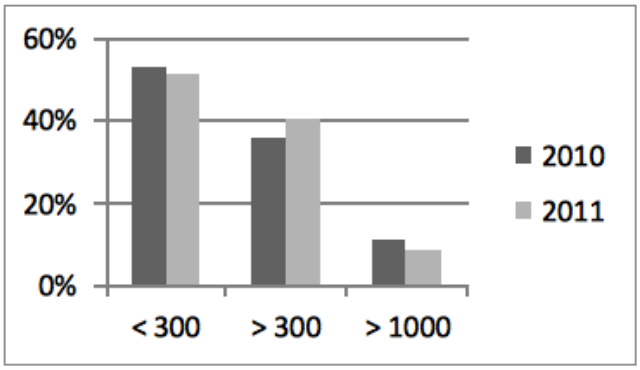
L'entità del danno patrimoniale subito, nel singolo caso, non è quasi mai elevata[2], attestandosi in prevalenza in misura non superiore a 300 euro (così in 240 casi su 455 nel 2010 e in 173 casi su 339 nel 2011); esborsi più consistenti,

1. In contrasto, tra l'altro, con quanto espressamente indicato dalle regole che *eBay* impone a chi intenda essere parte di quella particolare "*Community* di compravendita *online*". Tra quelle regole, infatti, è compreso il divieto di inviare "*email* contenenti offerte per comprare o vendere oggetti al di fuori del sito *eBay*", perché questo tipo di offerte presentano "un potenziale rischio di frode per i venditori e gli acquirenti" e, una volta che l'acquisto è stato effettuato "fuori del sito", non è più possibile beneficiare del "Programma di protezione acquirente di *eBay*", che consente il rimborso del denaro versato in caso di "oggetto non ricevuto o non conforme alla prescrizione".

2. Guardando il fenomeno dalla parte del gestore della piattaforma, i dati della Procura di Milano relativi al 2011 indicano che il totale dei danni subiti dalle vittime di truffa su *eBay* ammonta a circa



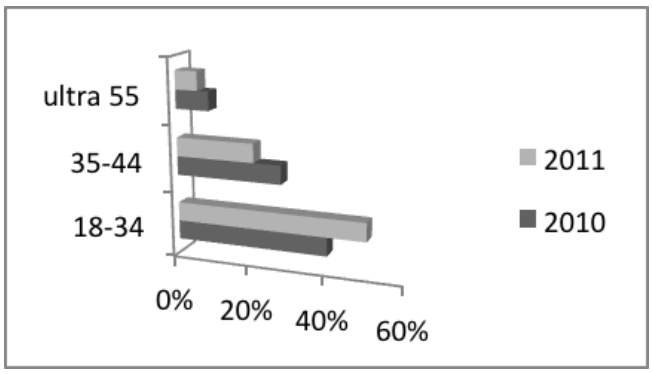
superiori a 1.000 euro — e talvolta anche a 5.000 euro — emergono in 51 delle denunce presentate nel 2010 (pari a poco più dell'11% dei casi) e in 29 di quelle del 2011 (corrispondenti all'8,5% del totale), relative alla compravendita di un motoveicolo o di un bene prezioso (ad es. un orologio di marca), così come nei casi di locazione di un immobile (per lo più ad uso turistico).



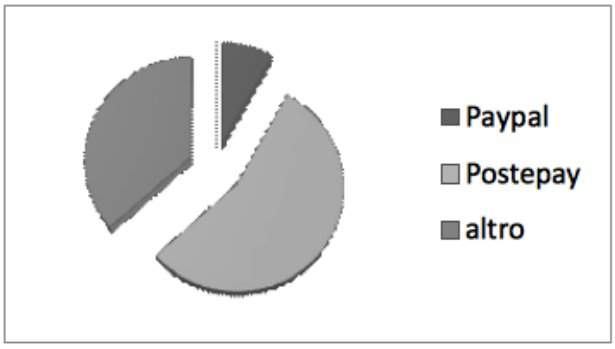
Vittime di questo tipo di truffa risultano essere persone di tutte le età, anche se si nota, nell'arco dei due anni oggetto di indagine, un sensibile aumento del numero di persone di età compresa tra i 18 e i 34 anni, che rappresentavano il 40% circa del totale nel 2010 e sono diventate poco più del 50% l'anno successivo. All'incremento della percentuale di vittime più giovani corrisponde evidentemente una diminuzione delle altre fasce di età, che nel caso delle persone tra i 35 e i 44 anni — che costituivano la fascia maggiormente colpita nel 2010 — appare particolarmente rilevante (dal 28% del 2010 si passa al 20,8% del 2011).

Quanto alle modalità di pagamento alle quali le vittime hanno fatto ricorso, la ricarica di una carta prepagata (per lo più la carta *PostePay*) è indicata in quasi la metà delle denunce (205 su 455 nel 2010 e 154 su 339 nel 2011); seguono i casi nei quali il pagamento è avvenuto tramite bonifico bancario, in una

150.000 euro. Una cifra significativa, se si pensa che *eBay*, presente in 39 mercati, con 124 milioni di utenti attivi al mondo (3,5 milioni solo in Italia), è uno dei più importanti siti di aste *on–line* e di commercio elettronico, che nel secondo trimestre del 2011 ha realizzato un utile mondiale pari a circa 600 milioni di dollari, derivante in buona parte dalle commissioni che i venditori privati e professionisti pagano, sia al momento dell'inserimento dell'offerta, sia alla conclusione della vendita.



percentuale che è andata aumentando, dal 23% del 2010 al 29,5% del 2011. In diminuzione sono i casi, già contenuti, nei quali è stato inviato del denaro attraverso un vaglia postale ovvero, laddove il beneficiario del pagamento fosse all'estero, utilizzando servizi di *money transfer* come *Western Union* o *Money Gram*[3]: questi casi rappresentavano complessivamente il 10% del totale nel 2010 e si sono ridotti intorno al 7% nel 2011.



Interessante è constatare che solo una esigua minoranza (44 casi su 455 nel 2010 e soltanto 17 su 339 nel 2011) ha fatto ricorso al sistema di pagamento *PayPal*, che il sito *eBay* indica agli utenti come affidabile e (tendenzialmente) garantito, a condizione che la compravendita si concluda sulla sua piattaforma: alle vittime della truffa tale sistema viene tuttavia presentato come troppo oneroso per le commissioni elevate che comporterebbe, proponendosi come alternativa proprio quei sistemi di pagamento (dalla ricarica della carta prepagata all'invio di denaro) che risultano pericolosi, perché del beneficiario si perde rapidamente ogni traccia.

2. Momento consumativo della truffa e competenza territoriale per le truffe *on–line*: orientamenti giurisprudenziali... Un primo problema nel

3. Quest'ultimo servizio presenta una serie di vantaggi, grazie all'accordo intervenuto tra *Money Gram* e Poste italiane, con il quale si consente ai titolari di un conto BancoPosta abilitato a BancoPosta *online* o di un conto BancoPosta Click di inviare denaro dal proprio *computer* senza alcun costo aggiuntivo. Cfr. *www.moneygram.com*.

quale ci si imbatte osservando il fenomeno delle truffe *on–line* è quello della individuazione del giudice territorialmente competente nei casi — che sono i più frequenti — nei quali la vittima procede al pagamento (anticipato) dei beni o servizi acquistati attraverso la ricarica di una carta *Postepay*. Caratteristica di questo strumento di moneta elettronica creato da Poste Italiane è infatti quella di essere una carta prepagata che non accede necessariamente ad un conto corrente — del quale sia possibile individuare il luogo in cui è stato costituito — e che può essere utilizzata dal titolare, per operazioni di prelievo o di pagamento nei limiti dell'importo disponibile, non solo presso qualunque ufficio postale o sportello automatico Postamat (e presso gli esercizi commerciali e gli sportelli automatici convenzionati con i circuiti internazionali), ma anche per via telematica, attraverso operazioni *on–line*[4]. Può risultare così difficile individuare il luogo di consumazione del reato nel singolo caso concreto, alla luce dell'orientamento prevalente in giurisprudenza, secondo il quale il reato di truffa si consuma "nel momento in cui si verifica l'*effettivo* conseguimento del bene da parte dell'agente e la definitiva perdita dello stesso da parte del raggirato"[5]. Poiché è la Carta — laddove manchi un conto corrente — ad essere oggetto di accredito in conseguenza della ricarica, il luogo nel quale il profitto viene effettivamente conseguito finisce col coincidere con quello nel quale essa è successivamente utilizzata e quindi « *con i tendenzialmente infiniti sportelli ATM (c.d. bancomat) sparsi sul territorio dello Stato o anche con lo stesso domicilio dell'indagato, dal momento che tali strumenti di pagamento sono utilizzati soprattutto* online »[6]. Una conclusione che renderebbe impossibile individuare il giudice competente attraverso il criterio generale della consumazione del reato indicato dall'art. 8 c.p.p. e imporrebbe di ricorrere a uno dei criteri residuali previsti dall'art. 9 c.p.p. e, in particolare, a quello incentrato nel luogo di residenza, domicilio o dimora dell'imputato o dell'indagato in forza dell'art. 61 c.p.p.

Di diverso avviso è, tuttavia, la Procura Generale presso la Corte di Cassazione che, dovendo dirimere conflitti di competenza in casi di questo

4. A partire dal 1° febbraio 2012 è stato introdotto il "Sistema Sicurezza *web Postepay*", che impone di abbinare un numero di cellulare ad ogni carta *Postepay* posseduta, per consentire la ricezione della *password* di autorizzazione (*One Time Password*) delle « *operazioni dispositive di ricarica Postepay, ricarica telefonica e pagamento bollettini effettuate con la carta Postepay sui siti di Poste Italiane* ». Questo sistema potrebbe agevolare l'individuazione del titolare della Carta — che spesso risulta ottenuta su presentazione di un documento falso — e prevenire l'indebito utilizzo sulla Rete di carte altrui.

5. Così Cass., Sez. un., 22 marzo 1969, P.m. c. Carraro e altro, in *Foro it.*, 1970, II, 5 ss., con nota di Boschi; nello stesso senso, Id., 30 novembre 1974, Forneris, in *Cass. pen.*, 1975, 751 ss., secondo la quale « *in tutte quelle situazioni in cui il soggetto passivo assume, per incidenza di artifizi o raggiri, l'obbligazione della dazione di un bene economico, ma questo non perviene, con correlativo di lui danno, nella materiale disponibilità dell'agente, si verte nella figura del reato di truffa tentata e non in quella di truffa consumata* », nonché Id., 21 giugno 2000, Franzo e altri, *ivi*, 2000, 3270 ss.

6. Così Cajani, *Aspetti giuridici comuni delle indagini informatiche,* in *Computer Forensics e indagini digitali*, a cura di Cajani, Aterno, I, Forlì, 2011, p. 198.

tipo, ha attribuito rilevanza — in modo del tutto condivisibile, ancorché in contrasto con l'orientamento prevalente in materia di truffa — al luogo nel quale la vittima ha subito il danno, anziché a quello nel quale l'agente ha conseguito il profitto. Di conseguenza, competente viene ritenuto il tribunale nella cui circoscrizione si trova l'ufficio postale presso il quale è stata effettuata l'operazione di ricarica della carta *Postepay*, « *giacché lì si verifica la* deminutio *patrimonii del soggetto passivo con contestuale arricchimento da parte dell'agente, arricchimento costituito dalla mera disponibilità e non già dall'effettivo utilizzo della somma* »[7].

Si sono così risolti i problemi di competenza, spostando l'attenzione sul momento (e sul luogo) nel quale la vittima ha compiuto l'atto di disposizione patrimoniale, ritenendosi che in questi casi danno e profitto si producano nello stesso momento, perché all'operazione di ricarica della Carta consegue in modo pressoché immediato una maggiore disponibilità di spesa per il titolare. Nelle ipotesi in cui il pagamento sia dalla vittima realizzato attraverso un bonifico bancario, e quindi « *con modalità di tempo e di luogo diverse (. . .) da quelle seguite con il pagamento effettuato con la ricarica delle carte prepagate* », la Procura generale mantiene invece ferma la competenza del giudice del luogo nel quale è stato acquisito l'ingiusto profitto, per effetto « *del positivo esito del disposto bonifico bancario* »[8]: essendo possibile identificare come luogo del conseguimento del profitto quello nel quale si trova il conto corrente oggetto di accredito, l'applicazione del criterio generale indicato dall'art. 8 c.p.p. non sembra incontrare ostacoli nella identificazione della consumazione della truffa con l'effettivo conseguimento dell'ingiusto profitto.

Eventuali problemi a dire il vero potrebbero sorgere nell'eventualità, tutt'altro che remota, che quel conto sia stato aperto presso un banca operante solo *on–line* — quindi senza sportelli sul territorio —, non potendosi in questo caso riproporre l'*escamotage* utilizzato per i casi di ricarica della carta *Postepay*: se è vero, infatti, che in conseguenza della ricarica danno e profitto si realizzano pressoché contestualmente, altrettanto non può dirsi — come la stessa Procura generale ha sottolineato — quando il pagamento è effettuato tramite bonifico bancario, stante l'intervallo temporale che di regola intercorre tra il momento nel quale viene dato l'ordine di trasferire il denaro e quello nel quale quest'ultimo viene accreditato. Lo 'spostamento' di competenza a favore del giudice del luogo dal quale la vittima ha disposto il bonifico implicherebbe in questi casi un'anticipazione del momento consumativo del reato (rispetto alla realizzazione del profitto), in

7. Così Procura Generale della Repubblica presso la Corte Suprema di Cassazione, Decr. N. 65/09 r.d. del 17 marzo 2009; nello stesso senso, Id., Decr. N. 228/10 r.d. del 5 luglio 2010; in precedenza, Id., Decr. n. 28/08 r.d. del 24 gennaio 2008.

8. Così Procura Generale della Repubblica presso la Corte Suprema di Cassazione, Decr. N. 254/09 r.d. del 29 ottobre 2009.

evidente contrasto con quanto richiesto dall'orientamento giurisprudenziale prevalente[9].

La risposta della Procura Generale ai conflitti di competenza per i casi di truffa *on–line*, nei quali la vittima ha effettuato la ricarica di una carta *Postepay*, non è tuttavia condivisa, vuoi per la difformità del criterio adottato rispetto a quello prevalentemente seguito dalla giurisprudenza per l'individuazione del momento consumativo della truffa, vuoi per le ripercussioni negative sul piano delle attività di indagine che essa sembra comportare: impedisce infatti la concentrazione presso uno stesso ufficio giudiziario delle denunce presentate nei confronti di uno stesso 'venditore', magari operante con nomi diversi e/o su piattaforme diverse. Data l'impossibilità, in cui si trovano gli uffici investigativi, di conoscere in tempo reale l'esistenza di altre denunce nei confronti della stessa persona, presentate presso una qualsiasi delle Procure della Repubblica del territorio nazionale, quel criterio rende più difficile pervenire « *all'accertamento dell'esistenza di una serialità nella commissione delle truffe* on–line »[10], che costituisce l'obiettivo prioritario nella complessa gestione di quella elevata percentuale di denunce contro ignoti che abbiamo in precedenza messo in rilievo.

Nella sua più recente giurisprudenza, tuttavia, la Procura Generale presso la Corte di Cassazione sembra essersi fatta carico di queste esigenze, risolvendo tendenzialmente i conflitti di competenza in favore dell'ufficio investigativo più prossimo all'indagato o comunque del luogo nel quale risulta esser stata posta in essere la condotta penalmente rilevante. Con riguardo, in particolare, ai casi di truffe *on–line* nei quali il pagamento è avvenuto attraverso la ricarica di una carta *Postepay*, si è ritenuto applicabile l'art. 8 c.p.p. individuandosi come luogo di consumazione del reato quello nel quale la carta è stata attivata e al quale quindi deve ritenersi "indirizzato" l'accredito della somma di denaro disposto dalla vittima, non diversamente da quanto avviene nei casi di bonifico bancario[11].

Si tratta senza dubbio di una soluzione che può in qualche modo rimediare alle difficoltà investigative che discendono da previsioni legislative inadeguate e che tuttavia, poggiando su una finzione (il collegamento territoriale tra la Carta e l'ufficio postale presso il quale è stata attivata), per di più non necessariamente risolutiva (quel luogo può essere del tutto estraneo

9. Nel senso che in questi casi non sembra opportuno identificare il *locus commissi delicti* con il luogo in cui si trova la sede legale della banca *on–line,* con conseguente attribuzione della competenza territoriale in modo pressoché esclusivo al Tribunale di Milano, Cajani, op. cit., p. 201 s.

10. Segnala questa esigenza Cajani, op. cit., p. 199, per il quale, nei casi di ricarica di una carta prepagata non abbinata ad un conto corrente, la competenza territoriale del giudice andrebbe individuata in base al criterio residuale indicato nell'art. 9, co. 2 c.p.p.

11. Cfr. Procura Generale della Repubblica presso la Corte Suprema di Cassazione, RG Decr. N. 64/2013 del 21 febbraio 2013 e Id., RG Decr. N. 171/2013 dell'11 aprile 2013. Lo stesso criterio è stato utilizzato in presenza di una imputazione per frode informatica, consistente nell'accredito abusivo di una carta prepagata: cfr. Id., RG Decr. N. 149/2013 del 27 marzo 2013.

all'agente), non consente di ritenere superato il problema.

3. . . . e possibili soluzioni *de lege ferenda*. Una risposta soddisfacente al quesito sulla competenza territoriale degli uffici giudiziari nei casi di truffe *on–line* non può non prendere le mosse da una critica all'orientamento giurisprudenziale ormai consolidatosi, secondo il quale il reato di truffa si consumerebbe nel momento e nel luogo in cui l'agente ha effettivamente conseguito il profitto ingiusto, essendo giunto in possesso del denaro che la vittima gli ha messo a disposizione per il pagamento dei beni o dei servizi acquistati[12]. Questa interpretazione trascura quella che è la peculiarità della truffa rispetto alle altre modalità di aggressione al patrimonio: la cooperazione della vittima al proprio depauperamento, attraverso il compimento di un atto di disposizione patrimoniale, in conseguenza dell'errore provocato dal comportamento fraudolento dell'agente. È nel compimento di quell'atto, del quale il profitto e il danno non sono che le dirette conseguenze, che va colto il disvalore della truffa e quindi il suo momento consumativo.

La scelta della giurisprudenza di posticipare tale momento fino al concreto manifestarsi degli effetti patrimoniali pregiudizievoli — benché « *il danno, tutto il danno penalmente rilevante, sia già nell'atto di disposizione* »[13] — viene giustificata con la necessità di rispettare la configurazione della truffa come reato di danno: un argomento che risulta tuttavia in contrasto con il dato, economicamente indiscutibile, che già con l'assunzione di un'obbligazione di dare il patrimonio della vittima subisce una diminuzione di valore (e quindi un danno), che appare fuorviante considerare in termini di mero pericolo.

Partiamo dunque dalla premessa che competente in materia di truffa, ai sensi dell'art. 8 c.p.p., è il giudice del luogo nel quale è stato compiuto l'atto di disposizione patrimoniale pregiudizievole con il quale la vittima, agendo all'interno della propria sfera patrimoniale, danneggia sé stessa a vantaggio del reo. Nell'ipotesi in cui tale atto consista nella ricarica di una carta prepagata (come la carta *Postepay*), competente è il giudice del luogo nel quale essa è stata effettuata, come giustamente ritenuto dalla Procura Generale della Cassazione: è in quel luogo infatti che il reato si è consumato, nessun rilievo assumendo il diverso momento e/o luogo nel quale il titolare della carta ha potuto beneficiare della somma accreditatagli. Qualora, invece, il pagamento sia avvenuto tramite bonifico bancario o postale, rilevante è il luogo dal quale è partito l'ordine di trasferimento della somma di denaro sul conto corrente indicato dal venditore.

12. Su questo aspetto si veda, diffusamente, Pecorella, *Truffe* on–line: *momento consumativo e competenza territoriale*, in *Riv. it. dir. proc. pen.*, 2012, 113 ss.

13. Così Pedrazzi, *Postilla circa la competenza per territorio in materia di truffa*, in *Riv. it. dir. proc. pen.*, 1958, ora in Pedrazzi, *Diritto penale*, vol. II, *Scritti di parte speciale*, Milano, 2003, p. 362.

Risulta a questo punto chiaro come, rispetto alle truffe *on–line,* questo criterio, coerente con la particolare fisionomia che il legislatore ha dato al reato di truffa, non consente quella concentrazione presso lo stesso ufficio giudiziario delle denunce nei confronti del medesimo venditore, dalla quale un'attività investigativa efficiente non può prescindere. Il problema, a ben vedere, sarebbe comune a tutti i casi di truffa — dal momento che questo reato si caratterizza per il ruolo determinante svolto dalla vittima —, ma sembra assumere una dimensione inaccettabile proprio nei casi di truffa *on–line*, nei quali le parti della compravendita non sono destinate ad incontrarsi in un luogo fisico, così che il luogo dell'atto di disposizione e quello del domicilio del venditore possano coincidere (come ci si aspetta che coincidano nella truffa). Al contrario, nella stragrande maggioranza dei casi le parti possono concludere ed eseguire il contratto restando ciascuna a casa propria, perché anche le modalità di pagamento dei beni sono cambiate: al versamento di una somma in contanti e, alla consegna di un titolo di credito si sono sostituite forme di pagamento a distanza che, grazie al collegamento tra i sistemi informatici, equivalgono, per la rapidità degli effetti, alla consegna di denaro nelle mani del beneficiario.

Quel criterio, peraltro, appare anche poco conforme alla *ratio* sottostante alla disciplina del codice di procedura penale nella quale si traduce la garanzia della precostituzione del giudice ai sensi dell'art. 25 co. 1 Cost.: secondo quanto dispone, come regola generale, l'art. 8 c.p.p., giudice 'naturale' del fatto è quello del *locus commissi delicti* perché la vicinanza con l'ambiente nel quale il reato si è realizzato dovrebbe rendere più agevole la raccolta delle prove e — si dice — consentire alla sentenza di condanna di svolgere al meglio la sua funzione dissuasiva[14].

L'importanza di radicare la competenza del giudice penale nel luogo in cui opera il reo — anziché in quello in cui si trova la vittima — emerge d'altra parte chiaramente dall'analisi delle diverse regole dettate in materia dal codice di procedura penale. Una 'deviazione' dalla regola generale è stata ad esempio introdotta per le ipotesi nelle quali il reato si consumi con la morte di una o più persone: in questi casi l'art. 8, co. 2 c.p.p. attribuisce la competenza al giudice del luogo in cui si è svolta la condotta, « *in considerazione della non infrequente sfasatura riscontrabile tra il luogo della condotta e quello in cui si verifica la morte della persona offesa* »[15]. Anche le regole suppletive, contenute nell'art. 9 c.p.p., individuano come rilevante il luogo della condotta ("il luogo in cui è avvenuta una parte dell'azione o dell'omissione"), se non addirittura, in subordine, il luogo di residenza, dimora o domicilio dell'imputato, a testimonianza di quanto sia importante

14. Cfr. Ricciarelli, *Trattato di procedura penale*, vol.1, tomo I, a cura di Dean, Torino, 2009, p. 62, nota 66 e autori *ivi* citati.

15. Così Della Casa, *Soggetti*, in *Compendio di Procedura penale*, a cura di Conso, Grevi, III, Padova, 2006, p. 16.

assicurare, ove possibile, la vicinanza del giudice all'ambiente nel quale si è manifestata la violazione della legge penale, o con il quale l'agente sembra avere un legame significativo.

Viene da chiedersi a questo punto se la *ratio* di quelle regole possa essere davvero rispettata quando il reato da giudicare sia stato commesso servendosi delle interconnessioni tra sistemi informatici e via sia quindi divergenza tra il luogo nel quale si è realizzata la condotta — e nel quale si trova l'elaboratore utilizzato dal reo — e quello nel quale si è verificata l'offesa, nella forma della lesione o della messa in pericolo del bene tutelato dalla norma incriminatrice: si pensi, oltre alle truffe *on–line*, ad alcuni reati informatici, come l'accesso abusivo a un sistema informatico (art. 615–*ter* c.p.), la violazione di corrispondenza informatica (art. 616 c.p.), il danneggiamento informatico (art. 635–*bis* e –*quater* c.p.), rispetto ai quali competente, in base all'art. 8 c.p.p., risulta essere il giudice del luogo nel quale si trova il sistema informatico violato o danneggiato: un luogo, il più delle volte, non solo diverso ma anche lontano da quello nel quale si è svolta la condotta del reo.

Problemi ancora più complessi sollevano poi le divere ipotesi nelle quali la condotta penalmente rilevante consiste nella diffusione, per via telematica, di notizie, immagini o programmi, dei quali sia per varie ragioni pericolosa la conoscenza o la disponibilità da parte di un numero indeterminato di persone: si pensi, ad esempio, al divieto di diffondere materiale pedo–pornografico (art. 600–*ter* c.p.), codici di accesso a un sistema informatico (art. 615–*quater* c.p.), programmi informatici diretti a danneggiare sistemi informatici (art. 615–*quinquies* c.p.), notizie false, idonee a provocare una sensibile alterazione del prezzo degli strumenti finanziari (art. 185 d.lgs. 58/1998)[16]. L'automatismo e la rapidità della comunicazione elettronica rendono sostanzialmente irrilevante quale momento si ritenga decisivo ai fini della consumazione del reato, tra quello dell'invio dei dati e quello della loro ricezione, da parte del sistema informatico; sensibilmente diverso può risultare invece il luogo in cui il reato si è consumato, a seconda che si privilegi il primo o il secondo momento, stante la possibilità che l'agente si trovi ad operare in un luogo diverso da quello nel quale è situato il sistema informatico destinatario della comunicazione. In situazioni di questo tipo, non solo si riscontra, ancora una volta, la necessità di assicurare che la competenza territoriale si radichi nel luogo nel quale o dal quale l'agente ha realizzato il reato, ma appare anche opportuno che le considerazioni relative al momento consumativo del reato non siano in qualche modo condizionate dalle conseguenze che sono in grado di produrre sulla competenza territoriale del giudice.

16. Sulla difficoltà di individuare il luogo di consumazione con riguardo all'aggiotaggio informativo, cfr. Consulich, *La giustizia e il mercato*, Milano, 2010, p. 343 ss.; da ultimo, in giurisprudenza, Cass., Sez. V, 4 maggio 2011, Tanzi e altri, in *Dir. pen. proc.*, 2011, 1096 ss., con nota di Mucciarelli.

Sembra dunque che vi siano valide ragioni per auspicare un intervento legislativo che, con riguardo ai reati che siano commessi a distanza, avvalendosi di un sistema informatico, individui la competenza territoriale del giudice attraverso un criterio diverso da quello incentrato sul luogo di consumazione del reato; soluzioni differenziate, del resto, sono state adottate in passato dal legislatore, di fronte alla accertata inidoneità dei criteri previsti in via generale dal codice di procedura penale.

Per quanto sin qui si è detto, pare opportuno che in questi casi la competenza territoriale venga radicata laddove la condotta esecutiva è stata posta in essere e quindi nel luogo nel quale si trova l'elaboratore elettronico del quale l'agente si sia servito per realizzare il reato; qualora quel luogo non sia individuabile nel singolo caso concreto — come spesso emerge dalle denunce dei casi di truffa *on–line* portate a conoscenza del Tribunale di Milano — non resterà che fare ricorso ai criteri sussidiari contemplati nell'art. 9 c.p.p. e quindi, in ultima istanza, competente potrà essere il giudice del luogo di residenza dell'imputato o dell'indagato.

4. La responsabilità del gestore della piattaforma informatica. Ulteriore aspetto problematico è quello della responsabilità del *provider* del quale non è facile tracciare contenuti e limiti. E ciò non solo perché si tratta di un tema complesso e delicato che si inserisce, specie negli ultimi anni[17], in un intenso dibattito dottrinale e giurisprudenziale[18], ma anche perché legislatore e interpreti si confrontano con una realtà magmatica, in continua evoluzione e sempre più difficile da ricomporre. A ciò si aggiunga che, in questo come in altri settori del diritto penale, si assiste ad un progressivo fenomeno di privatizzazione, che implica l'attribuzione a soggetti privati di compiti di prevenzione e gestione di ambiti tradizionalmente spettanti al potere punitivo statale[19]. Per queste ragioni, qui appena abbozzate, il tema si presta a distorsioni interpretative che sono il frutto di differenti concezioni di politica criminale.

Per quanto ovvia, una precisazione preliminare appare necessaria: la responsabilità del *provider* cambia a seconda dell'attività svolta[20]. Altro è consentire l'accesso alla rete o l'uso di una casella di posta elettronica; altro

17. Nella dottrina più recente cfr. Bartoli, *Brevi considerazioni sulla responsabilità penale dell'Internet service provider,* in *Dir. pen. proc.,* 2013, 600 ss.

18. V. Trib. Milano, 24 febbraio 2010, Drummond e altri, in *www.penalecontemporaneo.it,* 12 aprile 2010; sul punto v. Cajani, *Quella casa nella prateria: gli Internet Service Providers americani alla prova del caso Google Video, Nuove tendenze della giustizia penale di fronte alla criminalità informatica,* a cura di Picotti, Ruggieri, Torino, 2011, 216 ss.; Manna, *I soggetti in posizione di garanzia,* in *Dir. inf.,* 2010, 7, 779 ss.; App. Milano, 27 febbraio 2013, Drummond e altri, in *www.penalecontemporaneo.it,* 4 marzo 2013; sul punto v. Ingrassia, *La decisione d'Appello nel caos Google vs Vivi Down: assolti i manager, ripensato il ruolo del provider in rete,* in *Corr. merito,* 2013, 766 ss.

19. Cfr. Forti, *Democrazia economia e regolazione penale dell'impresa,* in *Dir. pen. proc.,* 2010, 773 ss.

20. Cfr. Luparia, *Il sistema penale ai tempi dell'internet. La figura del* provider *tra diritto e processo,* in Id., cit., 1 ss., il quale mette in rilievo « *la necessità di comprendere la tipologia concreta di sevizio che viene*

è gestire un *forum on–line* o un *social network*. La nostra analisi è circoscritta ad un ambito preciso e, quanto meno sul fronte penalistico, finora poco sondato: quello della compravendita di beni *on–line*.

Anche restringendo il campo d'indagine alla responsabilità del gestore di una piattaforma per il commercio elettronico, lo scenario risulta particolarmente complesso tanto in relazione alla realtà empirica, quanto al quadro normativo di riferimento.

La realtà di Internet appare ormai fatalmente cambiata rispetto a quella fotografata dal legislatore europeo. Le categorie di prestatori di servizi individuati dalla direttiva 2000/31/CE[21] sembrano del tutto anacronistiche e inadeguate. Nessuna delle tre attività descritte dalla direttiva — semplice trasporto (« *mere conduit* »)[22], memorizzazione temporanea (« *caching* »)[23] e memorizzazione (detta « *hosting* »)[24] — sembra coincidere pienamente con quella svolta dalle piattaforme di commercio elettronico. La prima sensazione (e forse non poteva essere altrimenti a quasi quindici anni di distanza) è che l'ampio panorama di servizi che rientrano nel c.d. *Web* 2.0 — *YouTube, Facebook, Twitter, Google, eBay*, ecc. — si trovino ad una distanza siderale rispetto alle categorie descritte dalla direttiva del 2000[25]. Ciò ha contribuito, in modo determinante, a rendere estremamente imprevedibili le decisioni giurisprudenziali, che sono state prese in un tessuto normativo, sia nazionale che sovranazionale, alquanto incerto e disomogeneo. Incertezza e disomogeneità che, quanto meno in relazione ai gestori di aste *on–line*, si sono moltiplicate in Italia a causa di un legislatore distratto e pasticcione.

Prima di analizzare più compiutamente le incertezze applicative che nascono da una legislazione incapace di interpretare l'evoluzione di Internet, occorre mettere in rilievo alcuni aspetti essenziali. Sono tre i profili che caratterizzano e facilitano la realizzazione delle truffe *on–line*. Oltre alla distanza fisica ed emotiva che separa autore e vittima e all'affidamento e alla fiducia che gli utenti normalmente ripongono nel gestore della piatta-

erogato quale presupposto essenziale per qualsivoglia valutazione in punto di addossabilità del rimprovero penale » (p. 6).

21. Sul punto v. Sieber, *Responsabilità penali per la circolazione di dati nelle reti internazionali di* computer. *Le nuove sfide di* Internet, in *Riv. trim. dir. pen. econ.*, 1997, 775 ss.

22. L'art. 12 della direttiva definisce tale attività come « *un servizio della società dell'informazione consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio, o nel fornire un accesso alla rete di comunicazione* »

23. L'art. 13 della direttiva definisce tale attività come « *un servizio della società dell'informazione consistente nel trasmettere, su una rete di comunicazione, informazioni fornite da un destinatario del servizio prestazione* » che effettua una memorizzazione automatica, intermedia e temporanea di tali informazioni effettuata al solo scopo di rendere più efficace il successivo inoltro ad altri destinatari a loro richiesta

24. L'art. 14 della direttiva definisce tale attività come « *un servizio della società dell'informazione consistente nella memorizzazione di informazioni fornite da un destinatario del servizio* »

25. Cfr. Flor, *Social networks e violazioni penali dei diritti d'autore. Quali prospettive per la responsabilità del fornitore del servizio?*, in *Riv. trim. dir. pen. econ.*, 2012, 647 ss.

forma, un ruolo determinante sembra giocarlo il sostanziale anonimato di cui godono i soggetti che operano sul mercato virtuale[26]. Ad esempio, per iscriversi ad *eBay* in forma completamente anonima è sufficiente utilizzare un indirizzo di posta elettronica e un nome di fantasia. Se poi si intende divenire venditori bisogna inserire un numero di carta di credito. A tal fine, con soli 10 euro si può attivare una carta ricaricabile *Postepay*, facendola intestare ad un'altra persona, attraverso l'esibizione di un documento d'identità falso o altrui, o anche il proprio, del quale poi si denuncerà falsamente lo smarrimento.

L'esigenza di tutela dell'anonimato, che in altri ambiti può prevalere all'esito di un bilanciamento di interessi (come nel caso in cui sia in gioco la libertà di manifestazione del pensiero), nel caso del commercio elettronico sembra affievolirsi fino quasi a scomparire. A ben vedere, l'esigenza di individuare gli operatori di un mercato virtuale interessa la sicurezza degli scambi commerciali prima ancora che il diritto penale. Per altro verso, è evidente che la tutela di acquirenti e venditori, dinanzi alla commissione di una truffa, presuppone la possibilità di identificare la controparte contrattuale.

In tal senso, la direttiva 2000/31/CE sul commercio elettronico stabilisce, tra le condizioni minime che gli Stati membri devono far rispettare al *provider,* che la persona fisica o giuridica per conto della quale viene effettuata la comunicazione commerciale debba essere chiaramente identificabile (l'art. 6, lett. *b*) e che « *il prestatore è comunque tenuto [. . .] a fornire senza indugio, a richiesta delle autorità competenti, le informazioni in suo possesso che consentano l'identificazione del destinatario dei suoi servizi con cui ha accordi di memorizzazione dei dati, al fine di individuare e prevenire attività illecite* » (art. 15, comma 2). Entrambe queste disposizioni sono contenute nel d.lgs. 9 aprile 2003, n. 70, con il quale la direttiva è stata recepita nel nostro Paese, agli artt. 8 e 17, co. 2.

Su un piano diverso ma complementare, ogni considerazione sulla responsabilità del *provider* nell'ambito del commercio elettronico deve prendere le mosse dagli artt. 14 e 15 della direttiva 2000/31/CE. Analogamente a quanto stabiliscono gli artt. 12 e 13 in relazione alle attività di semplice trasporto (« *mere conduit* ») e memorizzazione temporanea (detta « *caching* »), l'art. 14 introduce un'esenzione dalla responsabilità del *provider* che esercita attività di *hosting,* ossia quella che, in prima approssimazione, sembra meglio adattarsi al ruolo svolto dal gestore di un mercato *on–line*.

L'esenzione dalla responsabilità del prestatore di un servizio di memorizzazione di informazioni (c.d. *hosting*) opera, a condizione che quest'ultimo:

26. Cfr. Ingrassia, *Il ruolo dell'ISP nel ciberspazio: cittadino, controllore o tutore dell'ordine? Le responsabilità penali dei* provider *nell'ordinamento italiano*, in Internet provider *e giustizia penale. Modelli di responsabilità e forme di collaborazione processuale*, a cura di Luparia, Milano, 2012, p. 15 ss., 19; Petrini, *La responsabilità penale per i reati via internet,* Napoli, 2004, p. 69 ss., sul commercio elettronico in particolare p. 82 ss.

« *a) non sia effettivamente al corrente del fatto che l'attività o l'informazione è illecita e, per quanto attiene ad azioni risarcitorie, non sia al corrente di fatti o di circostanze che rendono manifesta l'illegalità dell'attività o dell'informazione, o b) non appena al corrente di tali fatti, agisca immediatamente per rimuovere le informazioni o per disabilitarne l'accesso* ». In base al secondo comma dell'art. 14 tale regime speciale della responsabilità « *non si applica se il destinatario del servizio agisce sotto l'autorità o il controllo del prestatore* ». L'art. 15 prevede, invece, l'assenza di un obbligo generale di sorveglianza in capo al *provider*. A prima vista la direttiva sembra restringere a tal punto la responsabilità di quest'ultimo, fino quasi a circoscriverla in ipotesi poco (o per niente) realizzabili. Ed allora il primo e fondamentale crocevia, attraverso il quale deve passare ogni considerazione sulla responsabilità del gestore di un mercato *on–line*, è rappresentato dalla domanda se in questo caso sia o meno applicabile la direttiva 2000/31/CE.

5. Gestore "attivo" vs. gestore "neutro": il chiarimento della CGUE. Se lo scopo della direttiva era « *di garantire un elevato livello di integrazione giuridica comunitaria al fine di instaurare un vero e proprio spazio senza frontiere interne per i servizi della società dell'informazione* »[27], il risultato disattende le aspettative. Come emerge da uno studio svolto per conto della Commissione europea nel 2007, la cornice legislativa teoricamente omogenea, che è contenuta nella direttiva 2000/31/CE, si è rapidamente frantumata non appena è entrata in contatto con gli ordinamenti degli Stati membri[28]. Sia pure in relazione a violazioni della proprietà industriale (vendita di beni contraffatti) commesse dagli utenti, la giurisprudenza dei vari Stati membri costituisce un valido punto di riferimento sia per mostrare l'incertezza nella quale si muovono gli operatori, sia per svolgere qualche considerazione in relazione alle truffe *on–line*. A tal fine basterà prendere in considerazione le soluzioni, talvolta diametralmente opposte, alle quali è giunta la giurisprudenza dei vari Stati membri.

Chiamato a valutare la responsabilità civile del *provider* per violazioni della proprietà industriale commesse dai propri utenti, il *Bundesgerichtshof* ha fissato, per la prima volta nel 2004[29], i criteri interpretativi ai quali si è poi conformata tutta la sua successiva giurisprudenza. Secondo la Suprema Corte tedesca *eBay*, in qualità di gestore di una piattaforma sulla quale utenti privati e venditori professionali possono vendere beni (all'asta), può avvalersi dell'esenzione dalla responsabilità prevista dall'art. 14

27. In tal senso si esprime il terzo Considerando della direttiva sul commercio elettronico.

28. Cfr. Inserire Autore, *Study on the internet liability of internet intermediaries, Markt/2006/09/E, Service Contract ETD/2006/IM/E2/69,* 2007, p. 30, nel quale si osserva che *« this report identifies common trends and crucial differences in the way that member states assess notions and concepts of liability for ISPs ».*

29. BGH, 11 marzo 2004, I ZR 340/01, in *Computer und Recht,* 2004, 763 ss. con nota di Volkmann, 1511 ss.

della direttiva 2000/31/CE, così come recepita dalla legislazione nazionale (*Telemediengesetz*).

Molto diversa risulta, invece, la situazione in Francia[30]. Per decidere se applicare l'esenzione dalla responsabilità di cui all'art. 14 della direttiva 2000/31/CE, come recepito dall'art. 6.1.2 della legge 21 giugno 2004 n. 575 (*Loi pour la confiance dans l'économie numérique*), la giurisprudenza (civile) guarda al ruolo in concreto svolto dal *provider.* Secondo il *Tribunal de grande instance* di Troyes, quando il gestore di un mercato *on–line*, in cambio di corrispettivo, mette a disposizione dei venditori strumenti per presentare e valorizzare i beni messi in vendita, stabilendo le regole di funzionamento e la struttura del servizio, allora il gestore della piattaforma deve essere ritenuto l'editore e non più semplicemente il prestatore di un servizio di memorizzazione (*hosting provider*)[31].

Nello stesso senso, la *Cour d'appel* di Parigi[32] ha rilevato che *eBay* fornisce assistenza ai venditori per ottimizzare le vendite, per descrivere gli oggetti messi in vendita e per creare uno spazio personalizzato di vendita. Non solo, *eBay* invia messaggi agli acquirenti per incitarli ad acquistare e per invitare chi non ha potuto vincere l'asta a guardare le offerte simili selezionate per lui da *eBay*. Per queste ragioni la Corte ha ritenuto che *eBay* non eserciti esclusivamente un'attività di *hosting*, ma svolga un ruolo attivo tale da conferirgli la conoscenza o il controllo dei dati immagazzinati sulla propria piattaforma e da escludere l'applicabilità dell'esenzione da responsabilità prevista dall'art. 6.1.2 della legge n. 575 del 2004 e dall'art. 14 della direttiva.

In senso parzialmente diverso il *Tribunal de grande instance* di Parigi[33] ha ritenuto che l'intero processo di vendita si svolga senza l'intervento del gestore, anche quando quest'ultimo offre strumenti tecnici per stilare l'offerta. La responsabilità circa la natura, il prezzo e la descrizione del prodotto rimane in capo al venditore, a meno che il gestore della piattaforma non abbia offerto altri servizi, come quello pubblicitario, che finirebbe per bloccare l'operatività dell'esenzione dalla responsabilità dell'*hosting–provider*.

Colta dai medesimi dubbi sulla responsabilità del gestore di un mercato *on–line*, la *High Court of Justice* di Inghilterra e Galles ha sollevato una questione pregiudiziale dinanzi alla Corte di giustizia dell'Unione europea.

Nel riprendere e approfondire le argomentazioni svolte in una preceden-

30. Per un quadro d'insieme aggiornato v. Bossan, *Le droit pénal confronté à la diversité des intermédiaires de l'internet,* in *Rev. sc. crim. dr. pén. comp.,* 2012, 295 ss.

31. Cfr. TGI, Troyes, 4 giugno 2008, *Hermes v. eBay,* in *juriscom.net;* analogamente cfr. T. Com. Paris, 30 giugno 2008, *LVMH v. eBay,* in *www.legalis.net*, con la quale *eBay* è stata condannata a risarcire 38,6 milioni di euro; sulla responsabilità civile del *provider* in Italia v. Trib. Milano, 23 marzo 2013, in *Leggi d'Italia*.

32. CA, Paris, 3 settembre 2008, *LVMH v. eBay,* in *www.legalis.net,* la cui sentenza è stata confermata da *Cour de Cassation*, 3 maggio 2012, in *www.legalis.net*.

33. TGI, Paris, 13 maggio 2009, *Lancome [L'Oréal] v. eBay,* in *www.legalis.net*.

te sentenza[34], la Corte nel 2011 individua il punto chiave per determinare il campo di applicazione del regime speciale di responsabilità delineato dalla direttiva. L'applicazione degli artt. 14 e 15 dipende dal tipo di ruolo — attivo o neutro — svolto dal gestore del mercato *on–line*. In particolare, « *laddove [...] detto gestore abbia prestato un'assistenza consistente segnatamente nell'ottimizzare la presentazione delle offerte di vendita di cui trattasi e nel promuovere tali offerte, si deve considerare che egli non ha occupato una posizione neutra tra il cliente venditore considerato e i potenziali acquirenti, ma che ha svolto un ruolo attivo atto a conferirgli una conoscenza o un controllo dei dati relativi a dette offerte. In tal caso non può avvalersi, riguardo a tali dati, della deroga in materia di responsabilità di cui all'art. 14 della direttiva 2000/31* » (v. punto 116 della sentenza)[35]. Sulla base di questa considerazione di carattere generale, la Corte di Giustizia rileva che « *l'art. 14, n. 1 della direttiva 2000/31 deve essere interpretato nel senso che esso si applica al gestore di un mercato on–line qualora non abbia svolto un ruolo attivo che gli permetta di avere conoscenza o controllo circa i dati memorizzati. Detto gestore svolge un ruolo siffatto allorché presta un'assistenza che consiste in particolare nell'ottimizzare la presentazione delle offerte in vendita di cui trattasi o nel promuoverle* » (punto 123)[36].

Quali conseguenze ha avuto o potrebbe avere la sentenza sulla giurisprudenza domestica in tema di responsabilità del gestore della piattaforma?

In Germania è stato osservato che, molto probabilmente, il *Bundesgerichtshof* dovrà rivedere la propria giurisprudenza fino ad ora monolitica[37].

A pochi mesi di distanza dalla sentenza della Corte di giustizia, la *Cour d'appel* di Parigi, nell'ambito di un procedimento penale a carico dell'ente, per i medesimi fatti di contraffazione all'origine della giurisprudenza civile già citata, ha condannato *eBay* ad un'ammenda di 200.000 euro — oltre alla pubblicazione della sentenza sul proprio sito per un mese e sui quotidiani *Le Monde* e *Le Parisien–Aujourd'hui* per sette giorni — per ricettazione di beni provenienti da delitto (contraffazione del marchio commessa dai propri utenti) di cui all'art. 321–1 del codice penale francese. Nel dare applicazione ai criteri interpretativi fissati dalla Corte di giustizia, la Corte d'appello di Parigi osserva che *eBay* non occupa una posizione neutra tra venditore e acquirente, ma gioca un ruolo attivo, offrendo ai propri utenti sia un servizio

34. CGUE, 23 marzo 2010, C–236/08, *Google France SARL e Google Inc. c. Louis Vuitton Malletier SA e altri,* in *curia.europa.eu*.

35. CGUE, 12 luglio 2011, C–324/09, *L'Oréal SA e altri c. eBay e altri,* in *curia.europa.eu*; v. van Eecke, Truyens, *L'Oréal v. eBay: The Court of Justice Clarifies the Position of Online Auction Providers,* in *Computer Law Review International,* 2011, 129 ss.

36. Sui problemi penalistici legati alla sentenza della Corte di Giustizia, cfr. D'Ambrosio, *Responsabilità degli* Internet Provider *e Corte di Giustizia dell'Unione Europea: quali spunti per il sistema penale italiano?*, cit., p. 67 ss. La distinzione tra *provider* attivo e passivo era già presente nella giurisprudenza italiana, anche se non in relazione al regime speciale di responsabilità di cui all'art. 14 della direttiva: v. Trib. Milano, 24 febbraio 2010, Drummond e altri, in *www.penalecontemporaneo.it*.

37. Rössel, *Filterpflichten des Provider im Lichte des EuGH,* in *Computer und Recht,* 2011, 589 ss.

di assistenza e gestione delle vendite, sia la possibilità di creare un negozio *on–line* e di divenire *"powerSellers"* (ossia uno dei migliori venditori che operano sul mercato *on–line* sia per volume delle vendite, sia per valutazioni positive degli acquirenti pari al 98%); ciò permette ai venditori di beneficiare di una serie di vantaggi ulteriori (offerte promozionali, *merchandising eBay* e programmi di formazione sulle migliori strategie di vendita). Il ruolo attivo di *eBay* è dimostrato altresì dal fatto che quest'ultima, nel prestare assistenza e nella promozione delle vendite, invia messaggi agli utenti per invitarli ad acquistare prodotti da lei stessa selezionati. Non si tratta, secondo la Corte, di una attività neutrale che si limita a ospitare le offerte dei venditori, ma di un'attività che si sostanzia in un contributo attivo. Contributo attivo che consiste nel promuovere le vendite dei prodotti dalle quali dipendono propri profitti[38]. Sulla base di queste considerazioni la Corte d'Appello di Parigi ha escluso l'applicazione del regime speciale della responsabilità previsto, in relazione all'*hosting provider,* dall'art. 6.1.2 della legge n. 575 del 2004 che ha recepito l'art. 14 della direttiva. Come emerge dalla ricostruzione dei fatti operata dalla sentenza, a partire dal 2004 i venditori hanno dato vita a un traffico di beni con marchio contraffatto, creando numerosi *account* attraverso l'uso di pseudonimi. Ciò ha reso ineffettive le contromisure adottate da *eBay* per porre fine alla violazione. Contromisure che, come nel caso della sospensione dell'*account*, vengono messe in atto solo dopo che *eBay* ha ricevuto almeno due o tre segnalazioni. Emerge qui nuovamente il ruolo fondamentale giocato dal sostanziale anonimato, del quale gli operatori del mercato *on–line* possono beneficiare nel commettere reati sulla piattaforma.

Solo nel 2006 l'intervento della polizia ha consentito di porre fine alle violazioni. Secondo la Corte, la passività nell'attività di sorveglianza e l'inefficacia delle contromisure adottate, da un lato, dimostrano che il gestore del mercato *on–line* non poteva ignorare l'attività fraudolenta realizzata dai propri utenti e, dall'altro lato, provano la volontà di *eBay* di preservare i propri interessi, evitando di sospendere gli *account,* al fine di non interrompere un'attività dalla quale trae profitto.

6. Truffe *on–line* e gestore del mercato: quali prospettive? Al di là della solo apparentemente facile distinzione, non priva di zone grigie, tra ruolo "neutro" o "attivo", che chiama in causa valutazioni altamente discrezionali dalle quali dipende il perimetro della responsabilità del gestore della piattaforma, nel sistema italiano è presente un vizio di fondo.

L'art. 18, co. 5 del d.lgs. 31 marzo 1998, n. 114 stabilisce che « *le operazioni di vendita all'asta realizzate per mezzo della televisione o di altri sistemi di comunicazione sono vietate* ». In base all'art. 22, co. 1 dello stesso decreto legislativo, la violazione di tale divieto è punita con una sanzione amministrativa pecunia-

38. CA, Paris, Pôle 5, chambre 12, 23 gennaio 2012, in *www.legalis.net*.

ria. A tale riguardo occorre rilevare che il Ministero delle attività produttive, con due circolari successive[39], ha precisato che « l'attività commerciale svolta nella rete Internet mediante l'utilizzo di un sito web (e–commerce), ove sia svolta nei confronti del consumatore finale e assuma la forma di commercio interno, è soggetta alla disciplina dell'art. 18 del d.lgs. 31 marzo 1998, n. 114 »[40]. A quanto consta, tale fattispecie di illecito amministrativo è stata applicata in un unico caso ad un sito d'aste *on–line* (*www.luccaste.it*) dal Sindaco di Lucca, con ordinanza poi confermata dalla Corte di Cassazione[41]. Le aste *on–line* rappresentano il 40% circa degli scambi su *eBay* (il 60% avviene a prezzo fisso)[42]; in questi casi, dunque, ci troviamo dinanzi ad un'attività illecita. Fatta questa premessa cerchiamo ora di analizzare gli eventuali profili di responsabilità del gestore del mercato *on–line* rispetto alle truffe commesse dai propri utenti, escludendo sin d'ora i casi in cui la sua attività sia rimasta del tutto neutra[43], e quindi soggetta alle deroghe alla responsabilità previste dagli artt. 16 e 17 del d.lgs. n. 70 del 2003, che hanno recepito in modo testuale gli artt. 14 e 15 della direttiva. L'art. 16 limita, infatti, in modo rigoroso i profili di responsabilità dell'*hosting provider,* ossia il gestore della piattaforma che rimane neutro. E lo fa in modo quasi del tutto preclusivo, salvo che ricorrano due ipotesi eccezionali: che il gestore neutro sia *effettivamente a conoscenza* del fatto che l'attività o l'informazione proveniente dall'utente–venditore è illecita oppure che il gestore non abbia agito immediatamente per rimuovere le informazioni o disabilitare l'accesso dell'utente, non appena sia venuto a conoscenza, su segnalazione delle autorità competenti, dell'attività illecita compiuta dall'utente. Come è stato rilevato, il requisito della 'conoscenza effettiva' circoscrive ulteriormente i già angusti spazi di responsabilità del gestore neutro: quest'ultimo sarà chiamato a rispondere solo « *ove il suo contributo quale partecipe o coautore sia sorretto almeno dal dolo diretto* »[44]. A ciò si aggiunga che l'art. 17 del d.lgs. n. 70 del 2003 esclude l'obbligo (generale) di vigilanza del gestore della piattaforma, come schermo dinanzi alla responsabilità omissiva. Se tale regime speciale di responsabilità vale per il gestore neutro del mercato *on–line* (i.e. l'*hosting provider*), diversa appare la situazione nella quale si trova lo stesso gestore quando assume, così come chiarito dalla Corte di giustizia europea, un ruolo attivo. Se si segue l'argomentazione della Corte di giustizia europea, in base alla quale

39. Si tenga presente che l'operazione interpretativa del Ministero era volta, specie nella seconda circolare, a circoscrivere l'ambito di applicazione dell'art. 18 d.lgs. n. 114 del 1998 solo ai commercianti al dettaglio.

40. Cfr. Circolare n. 3487/C del 1 giugno 2000 e n. 3547/C del 17 giugno 2002.

41. Cass. civ., Sez. II, 12 luglio 2005, n. 19668, in *Mass. Uff.*, n. 584389.

42. *Stampa.ebay.it*

43. In tal senso già si esprimeva Seminara, *La pirateria su* Internet *e il diritto penale,* in *Riv. trim. dir. pen. econ.,* 1997, 71 ss.

44. Ingrassia, *Il ruolo,* cit., p. 37.

deve ritenersi "attivo" il gestore che « *abbia prestato un'assistenza consistente segnatamente nell'ottimizzare la presentazione delle offerte di vendita di cui trattasi e nel promuovere tali offerte* », pare difficile non qualificare come attivo il suo contributo causale[45]. In questi casi, il *provider* non si è limitato a predisporre (in forma neutra) la piattaforma sulla quale ospitare le offerte dei venditori, ma ha offerto a questi ultimi un contributo ulteriore di assistenza e promozione. Ci troviamo dunque di fronte non alla mancata rimozione di un pericolo preesistente creato dal venditore sulla piattaforma, ma alla creazione di un pericolo nuovo (e quindi a una condotta attiva) da parte del gestore del mercato[46], attraverso un servizio di assistenza e gestione delle vendite, l'invio di messaggi agli utenti per invitarli ad acquistare prodotti selezionati oppure, più semplicemente, il rilievo dato sulla piattaforma ad una piuttosto che all'altra offerta (ad es. mediante il posizionamento). In questo caso, ossia quello che vede coinvolto il gestore attivo del mercato, non opera più il regime speciale di responsabilità previsto dal d.lgs. n. 70 del 2003. Sia pure nel ristretto ventaglio di ipotesi menzionate, sembra potersi affermare un contributo causale del gestore del mercato *on–line* alla realizzazione della truffa[47]. Questa considerazione non fa che aprire la strada ad una serie ulteriore di problemi difficilmente risolvibili. Il tema richiederebbe ben altro approfondimento. Ci si limita a segnalare che vi è, innanzitutto, la difficoltà di individuare la persona fisica che, all'interno della complessa organizzazione societaria della piattaforma informatica, è responsabile dei servizi offerti al venditore che rendono attivo il ruolo del *provider.* Il rischio è quello, come già accaduto in precedenza[48], di giungere a forme di responsabilità per posizione[49]. Altrettanto difficile pare l'accertamento del dolo — in questo caso anche in forma eventuale — in capo alla persona che gestisce i servizi di assistenza (gestione delle vendite; invio di messaggi agli utenti per invitarli ad acquistare prodotti selezionati; posizionamento sul sito internet degli oggetti in vendita, ecc.). A bene vedere, il diritto penale classico, che si rivolge alle persone fisiche, mal si adatta a questo tema. Anche se si arrivasse a ritenere penalmente responsabile un soggetto appartenente all'organizzazione, con il rischio più che concreto di violare, attraverso qualche forzatura

45. Cfr. Seminara, *La responsabilità penale degli operatori su internet,* in *Dir. inf.,* 1998, 745 ss.; Picotti, *Fondamento e limiti della responsabilità penale dei service–providers in internet,* in *Dir. pen. proc.*, 1999, 379 ss.; Id., *La responsabilità penale dei service–providers in Italia, ivi*, 1999, 501 ss.

46. Cfr. Fiandaca, *Riflessioni problematiche tra causalità e imputazione obiettiva,* in *Ind. pen.,* 2006, 951.

47. Cfr. Cass., Sez. III, 29 settembre 2009, Sunde Kolmisoppi e altri, in *Mass. Uff.*, n. 245935. Sia pure in relazione a violazioni del diritto d'autore, la Corte di cassazione ha ritenuto che l'indicizzazione costantemente aggiornata delle informazioni provenienti dagli utenti, per realizzare lo scambio tramite Internet di opere dell'ingegno protette da diritto d'autore, costituisce un apporto causale alla realizzazione del reato (p. 8 della sentenza).

48. Trib. Milano, 24 febbraio 2010, cit.

49. Cfr. Alessandri, *Diritto penale e attività economiche,* Bologna, 2010, p. 133 ss.

interpretativa, le garanzie fondamentali del diritto penale, non si risolverebbe certo il problema. Come è stato osservato, la punizione della singola persona fisica, « *quando possibile e qualunque cosa si pensi della pena, non riesce a chiudere definitivamente la vicenda nella sua sostanza* »[50]. In questo come in altri casi, rimangono da soddisfare standard minimi di tutela alle vittime. Tutela che non può certamente passare attraverso l'individuazione di un capro espiatorio. Ed allora l'unica strada percorribile sembra quella di coinvolgere l'ente, così come ha già fatto la più recente giurisprudenza francese (v. *supra* § 5), anche nella prevenzione delle truffe *on–line*. Per prevenire tali reati non è certamente sufficiente svolgere campagne informative rivolte agli utenti per "educarli" a gestire più consapevolmente i propri acquisti *on–line*[51]. La prevenzione presuppone, invece, l'inclusione delle truffe *on–line* tra le aree di rischio con le quali l'attività dell'ente si confronta.

A tal riguardo, vengono in rilievo due aspetti fondamentali che chiamano in causa l'organizzazione societaria del gestore del mercato on–line. Come si è visto, le contromisure messe in atto per fermare gli abusi rimangono del tutto ineffettive: non solo perché intervengono solo dopo due o tre segnalazioni[52], ma perché si confrontano con una platea di utenti che, agendo in forma anonima[53], dispongono di un numero elevato di *account*.

Il tema della responsabilità degli enti è estremamente complesso, specie con riguardo ai rapporti tra ricostruzione della colpevolezza del singolo e autonomia della responsabilità dell'ente[54]. In questa sede non ci si può che limitare ad abbozzare una proposta che va nella direzione di una più efficace tutela delle vittime di truffa *on–line*. In una prospettiva *de lege ferenda* parrebbe, quindi, opportuno allargare il catalogo dei reati presupposto previsti dal d.lgs. 8 giugno 2001, n. 231, che agli artt. 24 e 25–*bis*.1 comprende sia la frode nell'esercizio del commercio (art. 515 c.p.), sia la truffa aggravata (art. 640, comma 2 c.p.) e la frode informatica (art. 640–*ter* c.p.) « *se commessa ai danni dello Stato o di altro ente pubblico* », ma esclude la truffa. Dal momento che la fattispecie di cui all'art. 515 c.p. incrimina fatti meno gravi della truffa, che sono ugualmente caratterizzati da un (sia pur minimo) contenuto fraudolento[55], non si vede per quale motivo il legislatore abbia operato

50. Così Alessandri, *ult. op. cit.*, p. 211.

51. A tal riguardo si pensi alla guida elaborata da *eBay* e dall'Unione Nazionale Consumatori; v. *stampa.ebay.it*.

52. Cimino, *Sospensione dell'account di vendita nel marketplace di eBay, tutela del contratto e della libertà d'impresa,* in *Dir. inf.,* 2011, 121 ss.

53. L'individuazione degli autori di un reato è quasi sempre tecnicamente possibile. Ciò tuttavia chiama necessariamente in causa altri soggetti, quando invece dovrebbe essere già attuata dal gestore della piattaforma informatica.

54. Alessandri, *ult. op. cit.*, p. 222 ss.

55. Pedrazzi, *Errore e inganno nei delitti contro il patrimonio,* Milano, 1955, p. 87; ora in Id., *Diritto penale,* cit., p. 286.

questa frammentaria quanto irragionevole scelta di politica criminale.