

ROBERTO BARTOLI

LA FRODE INFORMATICA TRA « MODELLISTICA », DIRITTO VIGENTE, DIRITTO VIVENTE E PROSPETTIVE DI RIFORMA

SOMMARIO: 1. Considerazioni introduttive. — 2. Tutela del patrimonio e trasformazioni tecnologiche. — 3. I possibili modelli di tutela contro la frode informatica. — 4. Il modello vigente. — 5. Il modello vivente. — 6. Le prospettive di riforma. — 7. Considerazioni conclusive.

1. CONSIDERAZIONI INTRODUTTIVE.

Il presente contributo si articolerà in cinque parti. La prima sarà dedicata ad alcune considerazioni a carattere generale concernenti le trasformazioni subite dalle modalità di aggressione al patrimonio a séguito dello svilupparsi delle nuove tecnologie e, in particolare, delle tecnologie informatico-telematiche. Queste considerazioni serviranno per tratteggiare lo scenario di fondo all'interno del quale sarà poi compiuta la disamina della fattispecie di frode informatica. Nella seconda parte analizzerò la frode informatica in una prospettiva — per così dire — di politica criminale, avuto riguardo cioè ai possibili modelli di tutela a disposizione del legislatore al momento della previsione/configurazione della fattispecie contro siffatto fenomeno criminoso. In terzo luogo, esaminerò il modello di tutela vigente, adottato dal legislatore italiano nel 1993, al fine di individuare gli scopi che si è inteso perseguire e di verificare se la fattispecie introdotta sia stata configurata in modo coerente rispetto ad essi. La quarta parte sarà invece dedicata al modello di tutela vivente, così come delineato dalla giurisprudenza, e quindi alle principali questioni problematiche che si pongono sul piano applicativo, nel tentativo di compiere una sorta di dialogo con la stessa. Infine, nell'ultima parte formulerò alcune considerazioni in una prospettiva di riforma.

Le premesse di fondo di tutto il mio ragionamento sono due. Anzitutto, occorre aver chiaro che il legislatore italiano del 1993, e

* È il testo della relazione svolta al Corte Suprema di Cassazione, 8 aprile
Convegno *Il diritto penale della rete*, 2011.

ancor prima quello europeo del 1989¹, nell'alternativa tra una ricostruzione dei reati informatici come fattispecie prive di reale autonomia in quanto offensive di beni « classici » (patrimonio, fede pubblica, economia pubblica), oppure autenticamente « autonome », perché lesive di beni di nuovo conio come ad esempio l'intangibilità dei dati, si è mosso nella prima prospettiva, e quindi in una prospettiva che concepisce la dimensione « informatico-virtuale » in termini strumentali e accessori rispetto ad altre esigenze di tutela. In secondo luogo, e conseguentemente, si deve aver presente che, una volta intrapresa questa strada, da un punto di vista fenomenologico e tipologico la frode informatica può essere concepita basandosi sul modello della truffa oppure del furto. Se infatti, si adotta una visione — per così dire — *antropomorfica*, che identifica la macchina con l'uomo, si tenderà a incentrare il disvalore della frode informatica nell'inganno perpetrato ai danni dell'automa e quindi a forgiare un tipo criminoso sul modello della truffa. Se invece si adotta una visione *antropocentrica*, che pone al centro l'uomo e la sua attività, essendo indubbia l'unilateralità dell'aggressione della frode informatica, sarà fisiologico che la fattispecie si ispiri al tipo criminoso del furto, soprattutto se si incrimina il furto di energia elettrica e si attribuisce rilevanza anche alle modalità fraudolente.

Già da queste prime battute emerge in modo evidente come il « tipo » della frode informatica sia caratterizzato da una particolare ambivalenza e come assuma grande importanza la configurazione legislativa, in quanto, se il legislatore non è in grado di forgiare con la necessaria consapevolezza il tipo criminoso, si viene a creare il rischio che questa ambivalenza si tramuti in una vera e propria ambiguità, determinandosi così le condizioni per non orientare, o addirittura disorientare, la giurisprudenza. E come vedremo, ciò è proprio quanto accaduto nel nostro sistema penale [v. *infra*, § 5].

2. TUTELA DEL PATRIMONIO E TRASFORMAZIONI TECNOLOGICHE.

La prima considerazione a carattere generale che merita una certa attenzione riguarda la trasformazione subita negli ultimi decenni proprio dalle modalità aggressive della truffa e del furto: mentre rispetto alla truffa si è assistito a una sorta di spersonalizzazione delle forme lesive, per cui la cooperazione della vittima ha perduto progressivamente di valore e pregnanza, in ordine al furto si è verificato un procedimento per certi aspetti inverso,

¹ Si v. CONSIGLIO D'EUROPA, COMITATO DEI MINISTRI, Racc. n. R (89) 9, *Sulla cri-*

minaltà connessa agli elaboratori elettronici, 13 settembre 1989.

vòlto a valorizzare la relazione intercorrente tra la vittima e la cosa e quindi tra l'autore del reato e tale relazione.

In particolare, per quanto riguarda la truffa, il rapporto di cooperazione tra autore e vittima si è andato nel tempo sempre più allentando e sfilacciando. Ed infatti, in origine il disvalore della truffa si incentrava totalmente sulla cooperazione interpersonale, tant'è vero che la fattispecie poteva essere considerata a tutela della stessa libertà di disposizione della vittima, la quale veniva compromessa dagli artifici e dai raggiri e dal conseguente errore/inganno. Inoltre, il coinvolgimento — per così dire — personalistico della vittima si rifletteva su tutti gli eventi, ragion per cui alla condotta ingannatoria doveva conseguire non solo un errore, ma lo stesso atto di disposizione doveva essere posto in essere direttamente dallo stesso ingannato.

Successivamente si è manifestato un fenomeno di spersonalizzazione, sotto due diversi profili. Da un lato, si è verificata una spersonalizzazione derivante dalla trasformazione della vittima, la quale da soggetto specifico e ben individuato si è trasformata in un soggetto — per così dire — generico e impersonale come la pubblica amministrazione. Rispetto a questo fenomeno lo stesso oggetto della tutela della truffa ha subito una metamorfosi, venendo a consistere in una sorta di affidamento riposto dalla vittima nella veridicità e autenticità delle dichiarazioni dell'interlocutore, con interessanti conseguenze sul tipo, come ad esempio la minore centralità dell'errore e la possibilità di attribuire rilevanza giuridica all'atto dispositivo consistente in un'omissione. Dall'altro lato, si è avuta una spersonalizzazione a causa del progresso tecnologico, ragion per cui sono divenute sempre più ricorrenti le situazioni in cui l'autore non ha a che fare con una persona fisica, bensì con sistemi «meccanici». E a ben vedere, la stessa evoluzione legislativa ha seguito questi mutamenti, come dimostra l'introduzione nel 1990 della truffa aggravata ai danni dello stato (con successiva ulteriore specificazione nella indebita percezione di erogazioni a danno dello Stato) e nel 1993 della frode informatica.

Per quanto riguarda il furto, si è assistito invece a un processo inverso di valorizzazione della persona nella dinamica aggressiva. Se, da un lato, infatti, è indiscusso e indiscutibile il carattere spersonalizzato del tipo, non solo per la unilateralità dell'aggressione, ma anche per la possibile assenza di un rapporto diretto tra vittima e cosa mobile; dall'altro lato, però, altrettanto indiscussa è la tendenza ad attribuire rilevanza ad elementi che connotano una particolare relazione tra la vittima e la cosa mobile e quindi anche tra l'aggressore e la vittima. Si pensi in particolare alle riforme più recenti, tutte volte a valorizzare il rapporto esistente tra la vittima e la cosa o comunque modalità aggressive che hanno riflessi anche sul detentore: previsione del furto con strappo come fattispecie autonoma; introduzione delle nuove circostanze del

fatto commesso su mezzi di trasporto (art. 625, comma 1, n. 8-*bis*, c.p.) o nei confronti di persona che si trovi nell'atto di fruire o abbia appena fruito dei servizi di istituti di credito (art. 625, comma 1, n. 8-*ter*, c.p.). Ma si pensi anche all'incremento delle ipotesi in cui la relazione tra la vittima e il bene mobile sottratto si caratterizza per una sua persistenza, come nel caso della videosorveglianza.

Alla luce di queste considerazioni si può compiere una seconda considerazione sempre a carattere generale, ma più specificamente connessa al tema che stiamo trattando. Mentre il processo tecnologico risulta disfunzionale rispetto al tipo della truffa, al contrario la tecnologia non è disfunzionale al tipo del furto. In particolare, mentre la tecnologia rompe inevitabilmente la cooperazione tra autore e vittima caratterizzante la truffa; al contrario la tecnologia non altera il profilo della unilateralità dell'aggressione, incidendo piuttosto sulla configurazione dell'oggetto materiale e solo indirettamente sulla modalità della sottrazione, senza tuttavia eliminarne la componente della unilateralità.

Andando ancora più a fondo, rispetto al furto si può osservare come, se la tecnologia concerne gli strumenti di controllo da parte della vittima, si tende a valorizzare un modello di tutela del furto basato sulla relazione tra la vittima e la cosa mobile. Se, invece, la tecnologia riguarda la cosa mobile, il modello di furto che viene in gioco tende a basarsi sulla mera aggressione al patrimonio. Su questo aspetto si potrebbe indugiare a lungo. In particolare, merita porre in evidenza il diverso significato e la diversa portata di incidenza e condizionamento di un determinato fattore (es. trasformazione tecnologica) a seconda che incida sulla condotta oppure sull'oggetto materiale.

Terza e ultima considerazione a carattere generale. Per quanto riguarda la truffa, a questo processo di spersonalizzazione ha corrisposto una sorta di patrimonializzazione. Nella truffa il disvalore si è sempre meno incentrato sulle modalità della condotta e la catena vincolata degli eventi, per incentrarsi sempre di più sull'evento ultimo dell'ingiusto profitto con altrui danno. In buona sostanza, si è affermata sempre di più la tendenza a configurare la fattispecie in termini di reato a condotta libera, con conseguente danno al patrimonio altrui. Nel furto, invece, il discorso si fa leggermente più articolato. Da un lato, là dove la trasformazione tecnologica ha riguardato le modalità di relazione tra la vittima e la cosa, si è andati verso un rafforzamento della tutela di tale relazione e quindi il disvalore si è incentrato sempre più sulle modalità della condotta con conseguente personalizzazione e depatrimonializzazione del furto. Tant'è vero che, se per un verso, la giurisprudenza tende a non distinguere tra sottrazione e impossessamento anche quando esiste una relazione più o meno diretta tra la vittima e la cosa mobile, per altro verso, però, la giurisprudenza fa riferimento a quel concetto di « persistente vigilanza » che rivela

una valorizzazione di questa relazione, in piena coerenza con la distinzione tra sottrazione e impossessamento. Dall'altro lato, là dove la trasformazione ha riguardato soprattutto l'oggetto materiale, si è assistito invece a una spersonalizzazione e patrimonializzazione del furto.

Ecco allora spiegato perché il fenomeno della frode informatica finisce per porsi a metà strada tra la truffa e il furto in una prospettiva di complessiva spersonalizzazione e patrimonializzazione della tutela. Se infatti si fa riferimento al modello della truffa, ci si pone comunque nel solco di una sua concezione sempre più spersonalizzata e patrimonializzata. Ma anche se ci si ispira al modello del furto, dovendosi esaltare un diverso oggetto materiale « telematico », ci si colloca sulla scia che concepisce tale forma aggressiva ancora una volta in termini spersonalizzati e patrimonializzati.

3. I POSSIBILI MODELLI DI TUTELA CONTRO LA FRODE INFORMATICA.

Per quanto riguarda i modelli di tutela a disposizione del legislatore contro il fenomeno della frode informatica, preliminarmente occorre compiere due precisazioni — per così dire — in negativo. Anzitutto, le ipotesi di frode informatica non possono essere ricondotte alla fattispecie di truffa, anche là dove la truffa sia concepita in termini più lassi e aperti: non v'è dubbio, infatti, che manca la cooperazione di una persona fisica². D'altra parte, in secondo luogo, le ipotesi di frode informatica non possono essere ricondotte nemmeno alla fattispecie di furto, in quanto manca la cosa mobile suscettibile di sottrazione³. Certo si ha un arricchimento e un depauperamento, tuttavia tali risultati vengono conseguiti in forma informatica, telematica, nella sostanza virtuale.

In positivo, come accennato, la frode informatica può configurarsi secondo due modelli diversi⁴: secondo il modello della truffa, esaltando le analogie che sussistono tra l'inganno realizzato nei confronti della persona e l'inganno realizzato nei confronti della macchina; oppure secondo il modello del furto, esaltando l'unilateralità dell'aggressione che può avvenire anche mediante frode e le analogie che sussistono tra il furto di energia e l'uso non autorizzato di dati e più in generale di servizi informatico-telematici.

² In argomento v. per tutti C. PECORELLA, *Diritto penale dell'informatica*, Padova, 2006, 40 s., la quale precisa che « nei casi di manipolazione dei dati l'operatività della figura della truffa non poteva escludersi del tutto, ma risultava fortemente condizionata dalle circostanze del caso concreto ».

³ L. SCOPINARO, *Internet e reati contro il patrimonio*, Torino, 2007, 47.

⁴ In argomento cfr. A. DELLO IACOVO, *Art. 640-ter: truffa o furto? La frode informatica e il « modello 640 »*, in *Temi rom.*, 1997, 597 ss.

Il modello di frode informatica che si ispira alla truffa, proprio perché basato sulla valorizzazione delle analogie con la fattispecie a cooperazione della vittima, dovrebbe caratterizzarsi per una serie di eventi e per peculiari modalità di condotta⁵. Sotto il primo profilo degli eventi, a rigore, ne sarebbero necessari addirittura tre. Anzitutto, come la truffa si caratterizza per la realizzazione di un errore (inganno), anche la frode informatica si dovrebbe caratterizzare per la realizzazione di un errore (inganno) consistente in un risultato irregolare del processo di elaborazione di dati. Inoltre, come la truffa si contraddistingue per un atto di disposizione da parte del soggetto indotto in errore, così la frode informatica si dovrebbe caratterizzare per un atto di disposizione posto in essere direttamente dal sistema informatico o telematico. Infine, sempre al pari della truffa, nella frode informatica dovrebbero assumere rilevanza l'ingiusto profitto conseguito dall'autore e il corrispondente danno prodotto alla vittima.

Per quanto riguarda le modalità della condotta, come la truffa consiste in artifici e raggiri, la frode informatica dovrebbe consistere in una interferenza più o meno diretta sulle dinamiche informatiche e, più precisamente, in una manipolazione di dati o mediante interferenza sull'hardware o sul software (manipolazione indiretta) oppure mediante interferenza diretta sui dati (manipolazione diretta). Riguardo a quest'ultima modalità aggressiva di alterazione immediata si deve osservare come essa sia del tutto indifferente alla presenza o meno di un'autorizzazione alla elaborazione dei dati: è proprio la produzione della catena di eventi che rende irrilevante la questione della presenza o meno di un'autorizzazione all'esercizio di determinate attività. Detto diversamente, è la concentrazione del disvalore nella produzione di un ingiusto profitto con altrui danno che rende irrilevante l'esistenza o meno di un'autorizzazione ad elaborare determinati dati.

Per quanto riguarda il modello di frode informatica che si basa sul furto, ciò che si valorizza è l'unilateralità dell'aggressione con conseguente depauperamento della « vittima » e arricchimento dell'autore⁶. Le conseguenze che si hanno sul piano strutturale consistono nel ridimensionamento del ruolo degli eventi, *potendo* assumere rilevanza soltanto l'ingiusto profitto con altrui danno, e nella previsione di modalità di condotta consistenti nella interazione con il sistema operativo e, più precisamente, nell'uso di dati o servizi abusando o in assenza di un'autorizzazione.

In buona sostanza, mentre il modello basato sulla truffa incentra il disvalore sulla manipolazione diretta o indiretta di dati e su-

⁵ Cfr. C. PECORELLA, *Diritto penale dell'informatica*, cit., 63 ss.

⁶ A. DELLO IACOVO, *Art. 640-ter: truffa*

o furto?, cit., 604 ss.; L. SCOPINARO, *Internet e reati contro il patrimonio*, cit., 41 ss.

gli eventi, il modello fondato sul furto si incentra sull'interazione e sull'utilizzo illegittimo di determinati dati o servizi.

4. IL MODELLO VIGENTE.

Quale il modello adottato dal nostro legislatore? Prima di dare una risposta a questa domanda, si deve considerare che gran parte dei sistemi penali europei hanno finito per mettere assieme questi due modelli⁷. Ed infatti, in Paesi come la Germania, l'Austria e il Portogallo mentre, da un lato, sono previsti i tre eventi a cui abbiamo accennato in precedenza; dall'altro lato, sono state descritte tre diverse modalità e, più precisamente, oltre alla interferenza su hardware e software e alla manipolazione diretta di dati (quando c'è una manipolazione nei termini che abbiamo detto, non ha senso fare riferimento alla assenza di autorizzazione), è stato previsto anche l'uso di dati in assenza di un'autorizzazione.

Ebbene, a differenza di questi sistemi, quello italiano ha forgiato una fattispecie dai tratti molto ambigui⁸. In particolare, per quanto riguarda gli eventi, manca quello consistente nel risultato irregolare del processo di elaborazione di dati e quindi, conseguentemente e a rigore, dovrebbe mancare anche l'evento dell'atto di disposizione meccanico. Tuttavia, è presente l'evento dell'ingiusto profitto e dell'altrui inganno. Quindi si potrebbe dire che in ordine agli eventi la fattispecie si ispira per metà al modello del furto, là dove mancano gli eventi concernenti la macchina, e in parte al modello della truffa e del furto, là dove si prevede il profitto ingiusto con altrui danno.

Per quanto riguarda le modalità della condotta, anzitutto si fa riferimento ad espressioni « in qualsiasi modo » oppure « con qualsiasi modalità » davvero molto vaghe e dubbie. Si tratta di un profilo da non sottovalutare, in quanto, portando a confondere la generica descrizione di modalità della condotta, con l'assenza di una loro tipizzazione, ha indotto una parte della giurisprudenza e della dottrina a ritenere che si sarebbe in presenza di un reato a condotta libera⁹. In secondo luogo, ispirandosi al modello della truffa, la fattispecie prevede la condotta di « alterazione del funzionamento del sistema informatico o telematico », la quale di

⁷ C. PECORELLA, *Diritto penale dell'informatica*, cit., 64 ss.

⁸ C. PECORELLA, *Diritto penale dell'informatica*, cit., 67 s.; ID., *Art. 640-ter*, in E. DOLCINI e G. MARINUCCI (a cura di), *Codice penale commentato*, 2^a ed., vol. II, Milano, 2006, 4640; L. SCOPINARO, *Internet e reati contro il patrimonio*, cit., 44 ss.

⁹ Cass. pen., Sez. V, 24 novembre 2003, Noto, in *Giur. it.*, 2004, 2363, con nota di S. FERRARI, *Appunti in tema di frode informatica*, *ivi*, 2004, 2363 ss., anche in C.E.D., n. 4576/2004. In dottrina cfr. V. DESTITO, voce *Reati informatici*, in *Dig. disc. pen.*, Aggiornamento V, Torino, 2010, 753.

per sé non pone particolari problemi interpretativi, in quanto si tratta delle condotte di interferenza sull'hardware e sul software. Al contrario, pone problemi il riferimento all'«intervento senza diritto e con qualsiasi modalità su dati». Si tratta infatti di un'espressione alquanto ambigua perché non solo non distingue tra manipolazione (al di là dell'autorizzazione) e uso (connesso a questioni di autorizzazione), ma addirittura la fattispecie fa riferimento soltanto alla manipolazione (intervento su) e non anche all'uso. Inoltre, e soprattutto, la manipolazione, che di per sé dovrebbe essere del tutto indipendente dalla questione dell'autorizzazione, deve avvenire «senza diritto», in presenza cioè di una caratteristica che è coerente con la condotta di uso dei dati che invece non è prevista.

Alla luce di queste considerazioni si può allora concludere che la fattispecie si ispira al modello della truffa, là dove fa riferimento alla manipolazione, ma non si ispira a tale modello quando richiede che la manipolazione avvenga senza diritto e quando non si prevedono gli eventi del risultato irregolare del processo di elaborazione di dati e dell'atto di disposizione. Si ispira invece al modello del furto là dove non si prevedono eventi e si fa riferimento all'assenza di legittimità, ma non si ispira a tale modello quando omette il riferimento all'uso dei dati o comunque di un servizio.

5. IL MODELLO VIVENTE.

Nell'esaminare il modello vivente, mi pare opportuno distinguere tre diverse problematiche. Anzitutto, si sono poste questioni che addirittura sottendono una ricostruzione della frode informatica come ipotesi speciale di truffa. In questa prospettiva la frode informatica finisce per essere ricostruita come una vera e propria forma di truffa nella sostanza priva di reale autonomia sul piano del disvalore e, a ben vedere, frutto di quel procedimento di spersonalizzazione e patrimonializzazione a cui abbiamo accennato all'inizio e che contraddistingue il tipo di frode basato sulla truffa. In secondo luogo, vi sono questioni problematiche frutto della ambigua formulazione della fattispecie da parte del legislatore, e in argomento risulta interessante osservare come la giurisprudenza tenda a ricondurre alcune ipotesi di frode proprio alla fattispecie di furto. Infine, vi sono alcune questioni problematiche derivanti dalla presenza di vere e proprie lacune di tutela.

In ordine alla prime, si deve muovere dal fatto che per la prevalente giurisprudenza, confortata da una parte della dottrina¹⁰,

¹⁰ V. per tutti G. Ptica, *Diritto penale delle tecnologie informatiche*, Torino, 1999, 141 ss.

la fattispecie di frode informatica non sarebbe altro che un'ipotesi speciale di truffa. In argomento si è affermato che « la fattispecie tracciata ex art. 640-ter c.p. ha la medesima struttura e quindi i medesimi elementi costitutivi della truffa dalla quale si differenzia solamente perché l'attività fraudolenta dell'agente investe non la persona (soggetto passivo), di cui difetta l'induzione in errore, bensì il « sistema informatico » di pertinenza alla medesima, attraverso la manipolazione di detta persona »¹¹. In questa prospettiva, pertanto, la frode viene concepita come una sorta di fattispecie « speciale per specificazione » rispetto alla truffa di cui all'art. 640 c.p., dove al posto dell'inganno alla persona v'è soltanto l'alterazione del sistema informatico. Per il resto, sembra dire la Corte di Cassazione, la frode informatica è identica alla truffa.

Si tratta di un'interpretazione senza dubbio suggerita dalla formulazione ambigua della fattispecie e dalla previsione di un identico trattamento sanzionatorio per la truffa e la frode informatica, vale a dire da profili che non « inducono » ad uno sforzo ermeneutico orientato — per così dire — alla configurazione di un « tipo ». Tuttavia, essa desta non poche perplessità, in quanto pone le premesse per una ricostruzione del tipo di frode informatica poco rigorosa, con conseguente perdita di autonomia sul piano del disvalore e complessiva irrazionalità del sistema.

Ed infatti, quanto appena detto trova conferma rispetto a due questioni problematiche attinenti alla condotta di alterazione del sistema informatico e all'evento dell'atto di disposizione. In particolare, con riferimento alla condotta di alterazione, ci si deve chiedere se essa debba consistere nella mera alterazione « estrinseca » del sistema, senza conseguenze sui dati o sulla attività del programma, oppure in un'alterazione che incide più o meno direttamente sulla elaborazione dei dati o sulla attività del programma. Se si segue il primo orientamento è evidente che la frode informatica rischia di punire addirittura condotte prive di disvalore o comunque esprimenti un disvalore riconducibile ad altre fattispecie, mentre la seconda prospettiva è perfettamente coerente con un tipo di frode informatica che valorizza l'inganno realizzato ai danni della macchina¹². Ebbene, la giurisprudenza ha adottato la prima soluzione riconducendo alla fattispecie di frode informatica la

¹¹ Cass. pen., Sez. VI, 5 febbraio 2009, Giambertone, in C.E.D., n. 8755/2009; Cass. pen., Sez. V, 24 novembre 2003, Noto, cit.; Cass. pen., Sez. VI, 4 ottobre 1999, De Vecchis, in Cass. pen., 2001, 481 ss., con nota di L. ALESIANI, *Il momento consumativo del delitto di frode informatica: indicazioni contraddittorie della Cassazione*, ivi, 2001, 485 ss., anche in C.E.D., n. 3065/2000. Qualifica la frode

informatica come vera e propria truffa Trib. Palermo, 2 febbraio 2007, in *Giur. mer.*, 2008, 277 s., con nota di P. PERRI, *Analisi informatico-giuridica dei reati di frode informatica e accesso abusivo a un sistema informatico o telematico con l'aggravante dell'abuso della qualità di operatore di sistema*, ivi, 2008, 279 ss.

¹² In tale senso cfr. C. PECORELLA, Art. 640-ter, cit., 4635.

mera apposizione di una seconda scheda, vale a dire l'aggiunta di un software, all'interno di un sistema informatico costituente un impianto di gioco: «poiché la scheda originariamente contenuta nell'apparecchio così modificato era la sede del software del sistema informatico complessivo costituente l'impianto di gioco, è innegabile che la sostituzione di essa abbia comportato l'attivazione di un diverso programma e, per tal via, quella «alterazione del funzionamento di un sistema informatico» che la norma penale è finalizzata a reprimere. *Non rileva, cioè, il fatto che il software contenuto nella scheda originaria sia rimasto inalterato* [corsivo nostro] e possa operare regolarmente una volta riattivato: ciò che risulta alterato, nel caso in esame, è il funzionamento del sistema informatico nel suo complesso in dipendenza della sostituzione del software con altro diversamente operante»¹³.

D'altra parte, come accennato, si tratta di una soluzione che non ci sentiamo di condividere, perché il disvalore della frode informatica non può incentrarsi sulla mera alterazione di un sistema informatico, richiedendo necessariamente anche la conseguente manipolazione dei dati o interferenza sulla attività del programma. In buona sostanza, ogni condotta della frode informatica deve essere diretta in termini più o meno immediati alla manipolazione dei dati e alla interferenza sul programma. Con la conseguenza che se a séguito della condotta di interferenza il software o la sua attività restano inalterati, non si può parlare di vera e propria frode informatica, potendo il fatto eventualmente integrare altre ipotesi di reato.

Altra conseguenza si ha con riferimento all'interpretazione dell'atto di disposizione. Ci si chiede infatti se esso debba essere compiuto direttamente dalla macchina oppure anche da una persona fisica. Nella prima prospettiva, si tende a interpretare la fattispecie sul modello della truffa, ragion per cui all'inganno della macchina deve conseguire anche un atto di disposizione da parte della stessa¹⁴; nella seconda si tende invece a interpretare la frode informatica come ipotesi speciale di truffa in ordine al solo inganno perpetrato nei confronti della macchina, risultando invece tutti gli altri eventi nella sostanza identici a quelli della truffa. Ed anche rispetto a tale questione la giurisprudenza adotta la seconda soluzione: «il fatto che la manipolazione del sistema informatico alla fine possa determinare il compimento di un atto di disposizione patrimoniale da parte di una persona fisica non vale a cambiare la natura del reato»¹⁵. Tuttavia, si tratta di una soluzione che non può essere ac-

¹³ Cass. pen., Sez. V, 19 marzo 2010, Maselli, in C.E.D., n. 27135/2010.

¹⁴ I tal senso v. per tutti F. MUCCIARELLI, *Commento all'art. 10 della legge 547 del 1993*, in *Legisl pen.*, 1996, 138.

¹⁵ Cass. pen., Sez. II, 11 novembre 2009, Gabbriellini, in C.E.D., n. 44720/2009.

colta, in quanto fa venir meno la stessa ragion d'essere della frode informatica, visto che nel momento in cui c'è il coinvolgimento di una persona fisica, a monte c'è anche una induzione in errore, potendo trovare applicazione direttamente la truffa.

Venendo alle questioni problematiche derivanti dalla ambigua formulazione della fattispecie, assume rilievo l'inciso « senza diritto » riferito alla manipolazione dei dati¹⁶. In particolare ci si deve chiedere se una manipolazione senza diritto sia soltanto quella realizzata in assenza totale di autorizzazione (illegittimità — per così dire — già in astratto) oppure anche la manipolazione in mancanza parziale di autorizzazione (illegittimità — per così dire — in concreto). Classica ipotesi problematica è quella del dipendente di banca che s'impossessa mediante movimentazioni effettuate con i terminali dell'ufficio di somme di danaro di clienti depositate in conti correnti. Ebbene, se si ricostruisce la frode informatica sul modello della truffa, l'espressione « senza diritto » non può che essere interpretata nei termini più ampi possibili, talmente ampi da perdere nella sostanza di significato, con la conseguenza che possono integrare la fattispecie sia i soggetti del tutto estranei, sia quelli che avrebbero una autorizzazione in astratto, ma assente in concreto¹⁷. Se invece si asseconda la formulazione ambigua del legislatore e quindi si attribuisce un significato all'espressione « senza diritto » tale da dare rilevanza soltanto alle ipotesi in cui il soggetto agisce in totale assenza di un'autorizzazione, le ipotesi di manipolazione di dati in presenza di una illegittimità parziale finiscono per essere ricondotte alla fattispecie di furto.

E non è un caso che sul punto la giurisprudenza risulti divisa. Per un orientamento giurisprudenziale, infatti, l'ipotesi integra la fattispecie di frode informatica¹⁸. Altro orientamento riconduce invece il fatto all'interno del furto: « il delitto introdotto dalla norma da ultimo citata, infatti, prevede la condotta di chi, intervenendo in qualsiasi modo su un sistema informatico, ne alteri il funzionamento o ne manipoli i dati, informazioni o programmi, senza esserne autorizzato dal titolare del sistema. Nella specie, invece, il Rizzo non ha fatto altro che eseguire operazioni ordinarie sul sistema informatico della banca — quali gli ordini di bonifico da conto corrente —, alle quali era, dall'istituto titolare del sistema, personalmente abilitato »¹⁹. In sostanza, poiché la manipolazione deve avvenire senza autorizzazione, da intendersi come assenza assoluta di autorizzazione, in presenza di un'autorizzazione relativa si integra la fattispecie di furto.

¹⁶ Sul punto v. la lucida trattazione di L. SCOPINARO, *Internet e reati contro il patrimonio*, cit., 54 ss.

¹⁷ In tale senso v. G. PICA, *Diritto penale delle tecnologie informatiche*, cit., 146.

¹⁸ Cass. pen., Sez. V, 24 novembre 2003, Noto, cit.

¹⁹ Cass. pen., Sez. VI, 10 maggio 2007, Varriano, in C.E.D., n. 32543/2007.

A me pare da condividere la soluzione adottata dal primo orientamento, non solo — e non tanto — perché si finirebbero per espungere dalla fattispecie proprio le più classiche ipotesi di frode informatica, ma anche — e soprattutto — perché una volta previsto l'evento di ingiusto profitto con altrui danno e la condotta di manipolazione dei dati, non ha molto senso interrogarsi sulla autorizzazione o meno all'esercizio di determinate attività. Detto in altri termini, la soluzione che riconduce il fatto al furto, e che postula un'interpretazione della espressione « senza diritto » come assenza assoluta di autorizzazione, finisce per basarsi su un'interpretazione letterale dell'art. 640-ter c.p., tuttavia del tutto distonica rispetto a un tipo criminoso razionale ed omogeneo.

La terza categoria di questioni problematiche raccoglie ipotesi in cui sembra mancare nella sostanza una copertura legislativa. In particolare si tratta dell'uso abusivo di un servizio telematico e del c.d. furto di dati. In ordine al primo, il caso più diffuso e significativo concerne l'utilizzo fraudolento della telefonia. Posto che il sistema di telefonia mobile è qualificato pacificamente come sistema informatico, da un lato, si è formato un orientamento che qualifica il fatto in termini di frode informatica²⁰ o comunque di truffa²¹; dall'altro lato, si riconduce l'ipotesi in esame al furto, sulla falsa riga del furto di energia²².

Il nodo problematico è dato dalla circostanza che, per quanto riguarda la frode informatica, a ben vedere, manca una vera e propria manipolazione di dati, con la conseguenza che il fatto risulta atipico rispetto alla formulazione vigente della fattispecie di cui all'art. 640-ter c.p., che non contempla l'uso non autorizzato di dati; per quanto riguarda il furto, invece, a me pare che il flusso telematico possa essere legittimamente accostato al flusso di energia. Ecco allora che questa ipotesi potrebbe essere coperta dalla frode informatica, là dove si prevedesse come condotta anche quella di uso non autorizzato di dati o comunque di servizio telematico.

È interessante notare come ipotesi affini a quella dell'utilizzo della telefonia siano pacificamente qualificate come frodi. Così, ad esempio, in presenza di c.d. dialer truffaldini, si è ritenuta ap-

²⁰ Cass. pen., Sez. VI, 4 ottobre 1999, P.M. e Piersanti N., in *Cass. pen.*, 2000, 2990 ss., con nota di L. CUOMO, *La tutela penale del domicilio informatico*, *ivi*, 2000, 2298 ss., anche in *Foro it.*, 2000, II, 133, con nota di A. FANELLI, anche in C.E.D., n. 3067/1999; Cass. pen., Sez. VI, 4 ottobre 1999, De Vecchis, cit.; App. Milano, Sez. IV, 15 giugno 2001, in *Foro ambr.*, 2001, 339 s.; Trib. Lecce, 12 marzo 1999, Scognamiglio, in *Foro it.*, 1999, II, c. 608, con nota di A. FANELLI.

²¹ Cass. pen., Sez. I, 8 novembre 2005, Colucci, in C.E.D., n. 46541/2005.

²² Cass. pen. Sez. II, 21 dicembre 2004, Leonardi, in *Cass. pen.*, 2005, 3858 ss., con nota di A. TRIMBOLI, *Brevi note in tema di allacciamento abusivo a una linea telefonica: truffa o furto aggravato dal mezzo fraudolento*, *ivi*, 2005, 3860 ss., anche in C.E.D., n. 2349/2005; Cass. pen., Sez. II, 17 ottobre 2003, Di Mauro, in *Riv. pen.*, 2004, 403, anche in C.E.D., n. 47671/2003; tuttavia, di contrario avviso, Cass. pen., Sez. I, 21 dicembre 1977, Nucchi, in *Giust. pen.*, 1978, II, 440.

plicabile la frode informatica²³. Il dialer è un programma che, all'insaputa dell'utente, sconnette il modem dal provider ed attiva abusivamente un collegamento ad un altro erogatore di servizi tramite connessione telefonica ad elevata tariffazione. Parimenti è stata punita mediante frode informatica la clonazione di utenze radiomobili²⁴, la quale consente di addebitare a un'utenza telefonica i costi delle chiamate effettuate a mezzo di un altro apparecchio cellulare.

È tuttavia opportuno osservare come entrambe queste ipotesi risultino affini a quella di uso abusivo di un servizio soltanto perché concernenti la telefonia, rivelandosi invece molto diverse sul piano della condotta, visto che nei dialer truffaldini come nella clonazione c'è una vera e propria manipolazione di dati: nei primi, in forma indiretta, incidendo addirittura sul software; nell'ipotesi della clonazione, in forma diretta, alterando il numero di utenza e il numero seriale del proprio apparecchio telefonico.

Per quanto riguarda l'altra questione problematica della copiatura di dati, nonostante che una sentenza, per la verità piuttosto recente e di Cassazione, qualifichi il fatto come frode²⁵, la giurisprudenza di merito si esprime nel senso della irrilevanza²⁶. E quest'ultimo orientamento non può che essere condiviso mancando sia la condotta di alterazione²⁷, che l'evento di profitto.

Una battuta, infine, sul *phishing*²⁷. Com'è noto, tale fenomeno si compone essenzialmente di due fasi: con un inganno (spesso realizzato mediante falsa identità) si ottiene *username* e/o *password*; in seguito, utilizzando i dati carpiri, si compiono direttamente operazioni informatiche che consentono un indebito arricchimento. Ebbene, parte della giurisprudenza di merito, ritenendo che le due fasi possano essere tenute congiunte, conclude nel senso della configurazione della truffa, in concorso con altri reati, come ad esempio la sostituzione di persona²⁸. Tuttavia si tratta di una so-

²³ Trib. La Spezia, 23 settembre 2004, in *Giur. mer.*, 2005, 615.

²⁴ Cass. pen., Sez. II, 21 dicembre 2001, in *Foro ambr.*, 2002, 180; App. Milano, 15 giugno 2001, *ivi*, 2001, 339.

²⁵ Cass. pen., Sez. II, 14 settembre 2006, G.F., in *Dir. pen. proc.*, 2007, 363 ss., con nota di L. SCOPINARO, *Furto di dati e frode informatica*, *ivi*, 2007, 364 ss., anche in C.E.D., n. 30663/2006; Trib. Milano, Sez. III, 19 marzo 2007, in *De Jure*.

²⁶ Trib. Milano, Sez. III, 19 marzo 2007, cit.; Trib. Milano, 12 dicembre 2006, in *Giur. mer.*, 2007, 2048, con nota di F. RESTA, *Banche di dati on-line. I limiti della tutela penale*, *ivi*, 2451 ss.; Trib. Torino, 4 dicembre 1997, Zara, in *Giur. it.*, 1998, II, 1923.

²⁷ In argomento v. ampiamente R. FLOR, *Phishing, Identity theft e Identity abuse. Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. proc. pen.*, 2007, 899 ss.; nonché F. CAJANI, *Profilo penali del Phishing*, in *Cass. pen.*, 2007, 2294 ss.

²⁸ Trib. Monza, 7 maggio 2009, C.C.S., in *Riv. pen.*, 2010, 1300; Trib. Milano, 29 ottobre 2008, G., in *Corr. mer.*, 2009, 285 ss., con nota di F. ACNINO, *Computer crime e fattispecie penali tradizionali: quando il phishing integra il delitto di truffa*, *ivi*, 2009, 288 ss.; Trib. Milano, 15 ottobre 2007, in *Foro ambr.*, 2008, 69 ss., con nota di G. ARONICA, *Il «fishing» tra nuove esigenze di tutela ed acrobazie interpretative della giurisprudenza*, *ivi*, 2008, 74 ss.

luzione che suscita non poche perplessità, in quanto, a ben vedere, non solo si tratta di due episodi decisamente slegati, ma soprattutto la seconda fase si caratterizza per la totale assenza di collaborazione da parte della vittima. Più opportuno pertanto tenere le due fasi disgiunte e, là dove ne ricorrano tutti gli estremi, ricondurre la prima fase alla sostituzione di persona e la seconda alla frode informatica.

6. LE PROSPETTIVE DI RIFORMA.

Dalla disamina che abbiamo compiuto emerge in modo chiaro come la frode informatica prevista dal nostro ordinamento sia in realtà priva di una vera e propria «identità tipologica». Anzi-tutto, dalla giurisprudenza è concepita come un'ipotesi speciale di truffa, togliendole così autonomia sul piano del disvalore e attribuendo un ruolo del tutto estrinseco alla componente tecnologico-virtuale. In secondo luogo, è una fattispecie formulata in modo ambiguo e lacunoso, tale da non coprire tutte le ipotesi che dovrebbe, in quanto o una parte di esse finisce per essere ricondotta anche alla fattispecie di furto (manipolazione di dati in presenza di una autorizzazione «relativa») oppure addirittura risulta atipica (uso indebito di dati e loro copiatura). Non c'è dubbio quindi che si pone un'esigenza di riforma.

A questo punto si aprono due possibilità. Da un lato, si potrebbe tentare di tipizzare con più rigore il disvalore della fattispecie, sulla scia di quanto avvenuto in altri sistemi penale europei. Dall'altro lato, si potrebbe cogliere l'occasione per rimeditare in termini molto più approfonditi l'intero sottosistema dei reati c.d. informatici.

La prima strada consentirebbe di raggiungere un risultato immediato di non poco conto, e cioè di offrire un orientamento molto più chiaro e definito alla giurisprudenza che sembra trovarsi davvero smarrita. Tuttavia, essa rischia di essere molto miope. Ed infatti, un'esigenza di riforma non si avverte soltanto per la fattispecie di frode informatica, ma anche per tutte le altre fattispecie che prevedono reati informatici. In particolare, negli ultimi anni si manifesta sempre di più l'esigenza di superare una eccessiva frammentazione casistica dei reati informatici e di orientarsi verso una unificazione della tutela, anche perché questo eccesso di frammentazione ha finito per creare molti problemi interpretativi, derivanti soprattutto dalla interferenza tra fattispecie.

Ecco allora aprirsi la seconda strada, volta a vincere la frammentazione di un sistema che rischia comunque di appesantire l'attività interpretativa, nonché di non cogliere l'autentico significato di disvalore del fenomeno. Ma quali sono le cause di questa frammentazione? Essa sembra nascere da una sorta di legame dei reati informatici ai beni classici. Detto diversamente, come ac-

cennato all'inizio del presente contributo [v. *retro*, § 1], la riforma del 1993 si è ispirata a una concezione dell'informatica e della rete strumentale e servente rispetto a classiche esigenze di tutela, soprattutto a carattere patrimoniale. E così, in questa prospettiva, si è ritenuto che quella dei reati informatici non sia una categoria dai contorni omogenei, volta a tutelare un unitario bene giuridico, ricomprendendo invece al suo interno illeciti estremamente differenti tra loro, offensivi di interessi altrettanto diversi²⁹. Tuttavia, a ben vedere, sempre di più si coglie una certa autonomia dell'interesse informatico e della rete. Più precisamente, da un lato, si tende a non marcare troppo le differenze, come avvenuto rispetto al documento informatico con la recente riforma dell'art. 491-bis c.p. ad opera dell'art. 3, l. 18 marzo 2008, n. 48³⁰. Dall'altro lato, com'è stato lucidamente osservato già da tempo, «sarebbe riduttivo limitare il profilo offensivo [dei reati informatici] ai beni giuridici più tradizionali, come il patrimonio, la fede pubblica o l'economia pubblica, in quanto nessuno di essi, se isolatamente considerati, esaurisce la dimensione materiale delle offese realizzate dalla maggioranza degli illeciti informatici. Questi colpiscono tanto la conformità del fatto con la realtà, quanto il possibile profilo patrimoniale di tale relazione»; ecco allora che «si può proporre a tal fine la formula di "intangibilità informatica" la quale, in termini di astrazione normalizzatrice, indica la multiforme esigenza di non alterare la relazione triadica fra dato della realtà, rispettiva informazione e soggetti legittimati ad elaborare quest'ultima nelle sue diverse fasi (creazione, trasferimento, ricezione)»³¹, valorizzando così in termini autonomi la dimensione virtuale.

Ed un esempio di quanto appena detto è offerto proprio dalla frode informatica. Il suo ancoraggio al patrimonio non permette infatti di cogliere, sia nella formulazione italiana, sia in quella tedesca, il vero e proprio disvalore del fenomeno che si deve colpire, consistente anzitutto nella manipolazione del dato o nel suo indebito utilizzo, rispetto al quale è la causazione di danni patrimoniali a risultare eventuale e accessoria³².

Ecco allora che, in una prospettiva di riforma, si potrebbe pensare alla configurazione di fattispecie volte alla tutela della intan-

²⁹ In argomento v. per tutti L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in L. PICOTTI (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, 37 ss.; F. RESTA, *Virtualità del crimine. Dai reati informatici ai Cybercrimes*, in *Giur. mer.*, 2006, 104 ss.

³⁰ In argomento sia consentito rinviare a R. BARTOLI, *Le falsità documentali*, in

M. PELISSERO e R. BARTOLI (a cura di), *Reati contro la fede pubblica*, Torino, 2011, 178 ss.

³¹ V. MILITELLO, *Nuove esigenze di tutela penale e trattamento elettronico delle informazioni*, in *Riv. trim. dir. pen. econ.*, 1992, 374.

³² Per tali spunti si v. ancora V. MILITELLO, *Nuove esigenze di tutela penale*, cit., 373.

gibilità dei dati, che incriminano la loro manipolazione, sottrazione e uso indebito, prevedendo poi circostanze aggravanti là dove si vengono ad offendere anche altri beni.

7. CONSIDERAZIONI CONCLUSIVE.

Un'ultima battuta sui problematici rapporti tra legislatore e giudice. È noto come negli ultimi anni si sia riaperto un forte conflitto tra una visione fortemente legalista del diritto penale e una visione volta invece a valorizzare il ruolo del giudice. A me pare che quest'ultima visione sia difficilmente contrastabile, in quanto è — per così dire — nelle cose un tendenziale ed inevitabile incremento del ruolo del giudice. Ciò deriva non solo dalle « scoperte » dell'ermeneutica; non solo dall'esistenza di un sistema costituzionale basato su un controllo giurisdizionale di legittimità, sistema che determina una giurisdizionalizzazione del diritto sia per l'operato diretto della stessa Corte costituzionale, sia per l'attività interpretativa costituzionalmente orientata dei giudici; ma anche per la diffusa sciatteria legislativa che impone al giudice di ricostruire tipi criminosi omogenei, nonché per la trasformazione dei fenomeni criminosi, rispetto ai quali il legislatore si trova costantemente in ritardo (si pensi alla evoluzione della corruzione, della contraffazione etc.). Da qui una giurisprudenza che cerca di offrire risposte alle esigenze sociali in continua evoluzione, ponendosi a quel punto inevitabilmente in tensione con una previsione legislativa nella sostanza superata dalla realtà. E la fattispecie di frode informatica, con la sua formulazione ambigua e lacunosa, mette in evidenza proprio questa inevitabile valorizzazione del ruolo della giurisprudenza a séguito della sciatteria e dell'inerzia legislativa.

D'altra parte, dalla disamina del diritto vivente sono emerse anche « responsabilità » nell'operato della giurisprudenza, a volte sofferente di una certa accidia. In particolare, destano notevoli preoccupazioni la ricostruzione della frode informatica come ipotesi speciale di truffa e l'interpretazione letterale dell'espressione « senza diritto », vale a dire l'adozione di opzioni ermeneutiche che lasciano trasparire un atteggiamento culturale della giurisprudenza penalistica italiana ancora restia ad appropriarsi in modo consapevole del concetto di « tipo criminoso ».