5/2018

LA TUTELA PENALE DELL'IDENTITÀ DIGITALE

di Chiara Crescioli

SOMMARIO: 1. L'identità digitale e il furto d'identità. – 2. Il furto d'identità digitale nella giurisprudenza. – 3. Il nuovo terzo comma dell'art. 640-*ter* c.p. e il tentativo del legislatore di colmare il vuoto normativo. – 4. Brevi considerazioni conclusive.

1. L'identità digitale e il furto d'identità.

La popolarità e l'utilizzo tra il pubblico del mezzo *Internet* hanno comportato la creazione di milioni di identità digitali, al fine di svolgere in questo spazio virtuale le attività più disparate.

Si possono individuare diverse tipologie di identità digitali, in relazione alle attività da compiere sul *web*[1], motivo per cui la nozione di identità digitale è comunemente intesa secondo due differenti accezioni, ovvero sia come rappresentazione nel mondo *online* di una persona fisica o giuridica, sia come insieme delle informazioni e delle risorse concesse da un sistema informatico al suo utilizzatore o, meglio, come l'insieme di codici elettronici attribuiti ad un soggetto fisico, che ne consentono l'identificazione nel mondo virtuale[2].

Ma in *Internet* cambiare o acquisire un'identità nuova o altrui anche per scopi illeciti è estremamente facile: i dati sul c.d. furto d'identità digitale, oggi riconducibile al più vasto fenomeno globale del *cybercrime*[3], sono allarmanti[4], essendo emersa l'esistenza

---

[1] Alcune, necessarie per accedere a determinati servizi pubblici o utilizzate per compiere operazioni di particolare importanza, vengono rilasciate dai gestori agli utenti richiedenti a seguito di una procedura volta ad identificare questi ultimi. Altre, quali ad esempio la creazione di una casella di posta elettronica, sono create direttamente dal soggetto stesso, che può scegliere il nome da utilizzare nella rete.

[2] M.F. COCUCCIO, *Il diritto all'identità personale e l'identità "digitale"*, in *Dir. fam. e pers.*, 2016, n. 3, p. 949 ss., p. 954.

[3] La distinzione tra *computer crime* e *cybercrime* nel passaggio all''*epoca di Internet*', in cui il *cyber space* è diventato l'ambiente ideale e privilegiato per la realizzazione di molteplici reati, è descritta da L. PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in ID. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, p. 21 ss., p. 29. Per una precedente panoramica sui reati informatici v. L. PICOTTI, *Reati informatici*, voce in *Enciclopedia giuridica*, Volume di aggiornamento VIII, Treccani, Roma, 2000, p. 1 ss., *passim.*

[4] Cft. i dati resi noti dalla Centrale Rischi Finanziari (CRIF) nella sua *Smart Research sul furto d'identità*, Bologna, 2014, nella quale l'Osservatorio istituito da CRIF ha effettuato una stima di 25.300 casi verificatisi nel nostro Paese nell'intero anno 2015, con una perdita economica complessiva superiore ai 172 milioni di Euro.

anche di vere e proprie associazioni a delinquere, che si dedicano alla vendita ed allo scambio dei dati personali altrui illecitamente ottenuti[5].

Il furto d'identità digitale è un fenomeno criminoso prodromico alla commissione di ulteriori illeciti, che si articola in diverse fasi, ovvero: l'ottenimento delle informazioni personali della vittima, l'interazione con le informazioni personali, che consiste nel possesso e nella vendita di tali dati, e l'utilizzo delle informazioni personali illecitamente ottenute per commettere ulteriori reati, non necessariamente contro il patrimonio, ma anche ad esempio diffamazioni o minacce[6].

Le tecniche con le quali vengono carpite le informazioni personali delle vittime sono molteplici e col passare del tempo sono diventate sempre più sofisticate. Oltre alle tecniche c.d. tradizionali, quale ad esempio il furto di una carta d'identità, la tecnica maggiormente utilizzata e conosciuta è sicuramente il *phishing*, che consiste nell'invio di e-mail abilmente contraffatte, che segnalano all'utente inesistenti problemi al *server* dell'istituto bancario o la necessità di aggiornare i propri dati, per indurre l'utente stesso a cliccare su un apposito *link* in cui gli viene richiesto di fornire i propri codici identificativi[7]. A questo *phishing* c.d classico si aggiungono poi moltissime varianti quali il *phishing* basato su *malware*[8], il *phishing "man-in-the-middle* [9], lo *Smishing* e il *vishing*[10], ecc. Un'evoluzione del *phishing* è il *pharming*: in questo caso la vittima è invitata a fornire le proprie generalità con la diversa e più sofisticata tecnica del sito "clone" di quello ufficiale[11].

2. Il furto d'identità digitale nella giurisprudenza.

Il furto d'identità digitale non è previsto nell'ordinamento italiano come reato autonomo.

---

[5] Così come riportato da Cajani in F. CAJANI – G. COSTABILE – G. MAZZARACO, *Phishing e furto d'identità digitale. Indagini informatiche e sicurezza bancaria,* Milano, 2008, p. 188.

[6] F. CAJANI, *La tutela penale dell'identità digitale alla luce delle novità introdotte dal d.l. 14 agosto 2013, n. 93 (convertito con modificazioni dalla l. 15 ottobre 2013, n. 119),* in *Cass. pen.*, 2014, n. 3, p. 1094 ss., p.1096

[7] Per un approfondimento sul tema v. R. FLOR, *Phishing, identity theft e identity abuse. Le prospettive applicative del diritto penale vigente,* in *Riv. it. dir. proc. pen.*, 2007, n. 2-3, p. 899 ss., p. 900.

[8] V. Cajani in F. CAJANI – G. COSTABILE – G. MAZZARACO, *Phishing e furto d'identità digitale,* cit., p. 28 s.: il *phisher* intercetta i messaggi indirizzati ad un sito scelto da qualsiasi utilizzatore, salva le informazioni che gli interessano, poi trasmette i messaggi al sito scelto dalla vittima ed infine inoltra le risposte di ritorno.

[9] In questo caso l'*e-mail* di *phishing* contiene un *link* c.d. "maligno" che una volta scaricato danneggia o altera i dati informatici presenti nel computer. Sul punto v. OECD, *Scoping Paper on Online Identity Theft*, OECD, *Scoping Paper on Online Identity Theft*, Seul, 2008, disponibile *online* al sito www.oecd.org/dataoecd/35/24/40644196.pdf, p. 16.

[10] Ovvero *phishing* commesso tramite SMS o mediante telefono. Per un maggiore approfondimento v. P. PERRI, *Lo smishing e il vishing, ovvero quando l'unico limite all'utilizzo criminale delle nuove tecnologie è la fantasia,* in *Dir. Internet,* n. 3, 2008, p. 266

[11] V. OECD, *Scoping Paper on Online Identity Theft*, op. cit., p. 19: nel *computer* del malcapitato viene inserito un *virus* che modifica la lista dei siti contrassegnati come preferiti nel *browser* utilizzato dalla vittima, che viene quindi reindirizzata su un sito "clone" di quello dell'istituto di credito o dell'istituzione, ed attraverso il *login* a quest'ultimo vengono intercettate le sue credenziali.

Un primo orientamento giurisprudenziale della Cassazione in materia di furto d'identità, ritenendo che questo fenomeno criminoso ledesse il diritto alla riservatezza ed in specie ad esprimere il necessario consenso in materia di trattamento di dati personali, lo ha ricondotto al reato di trattamento illecito di dati personali, previsto dall'art. 167 d.lgs. 30 giugno 2003 n. 196[12].

L'orientamento della Cassazione è in seguito mutato. Avvalendosi dello strumento dell'interpretazione estensiva[13], la Suprema Corte ha ricondotto alla fattispecie di cui all'art. 494 c.p.[14] le nuove forme di aggressione dell'identità digitale, che comportino come conseguenza un danno incidente su una sfera diversa da quella patrimoniale della persona offesa[15]. Nella prima pronuncia in materia del 2007, la Cassazione ha enunciato il principio di diritto per cui il bene giuridico della pubblica fede ben può essere leso da inganni anche commessi su *Internet* relativi alla vera essenza di una persona, alla sua identità o ai suoi attributi sociali[16]. Tale orientamento giurisprudenziale è stato condiviso dalla dottrina, che ha correttamente ritenuto che le falsità personali siano caratterizzate dal contenuto della rappresentazione e non dalla forma[17].

In una successiva pronuncia del 2012 la Cassazione ha poi stabilito che l'esigenza di tutela dei soggetti ed il principio personalistico riconducibile all'art. 2 Cost. impongono che tra i segni distintivi della persona si includa anche il *nickname*[18]. La

---

[12] V. Cass pen., sez. III, 26 marzo 2004 n. 28680: il caso riguardava un uomo che aveva diffuso su un sito *Internet* le immagini registrate in una videocassetta contenente lo spogliarello della *ex* fidanzata, pubblicando anche il suo numero di cellulare, così simulando la sua disponibilità ad incontri di natura sessuale. V. anche Cass. pen., sez. III, 17 novembre 2004, n. 5728 in *Dir. pen. proc.*, n. 4, 2006, p. 464 ss. con nota di I. SALVADORI, *Il trattamento senza consenso di dati personali altrui reperibili su Internet costituisce reato?* Il secondo caso riguardava un uomo che aveva aperto a nome di una giocatrice della nazionale di pallacanestro un sito *internet*, utilizzato illecitamente i suoi dati per iscriverla ad un sito di messaggeria erotica e pubblicato a suo nome un messaggio di analogo contenuto.

[13] In argomento, sulla distinzione dall'analogia in *malam partem*, vietata in materia penale cft. per tutti F. ANTOLISEI, *Manuale di diritto penale, PG*, VIII ed. revisionata da L. Conti, Milano, 1980, p. 66; F. MANTOVANI, *Dir. pen., PG*, IX ed., Padova, 2015, p. 73.

[14] V. P. ASTORINA MARINO, Sub. *art. 494 c.p.*, in *Commentario breve al codice penale*, diretto da G. Forti, S. Seminara, G. Zuccalà, VI ed., Padova, 2017, p. 1652 ss., p. 1654.

[15] F. CAJANI, *La tutela penale*, cit., p. 1096

[16] V. Cass. pen., sez. V, 8 novembre 2007, n.46674: la vicenda riguardava un uomo che, dopo aver creato un *account* di posta elettronica a nome di un'amica e fornito anche il suo numero di cellulare, lo utilizzò per simulare la disponibilità della donna a prendere parte ad incontri sessuali ed indusse più uomini a telefonarle.

[17] C. FLICK, *Falsa identità su internet e tutela penale della fede pubblica degli utenti e della persona*, in *Dir. inf. inf.*, 2008, n.4-5, p. 526 ss., p. 531 ss.

[18] V. Cass. pen., sez. V, 28 novembre 2012, n.18826: in questo caso una donna, partecipando con un *nickname* ad una *chat* di carattere erotico, aveva fornito agli altri utenti il numero di cellulare apparentemente proprio, ma in realtà della sua *ex* datrice di lavoro, la quale aveva ricevuto telefonate e messaggi SMS indesiderati da parte di uomini che la credevano disponibile ad incontri di natura sessuale. Secondo la Corte non rilevava affatto che il nomignolo registrato nella banca dati della *chat* erotica, che conteneva le iniziali della donna, fosse inventato e che alla vittima non lo avesse mai impiegato quale segno distintivo, dato che lo stesso contribuiva a renderlo chiaramente riconducibile ad una persona in carne ed ossa, e concorreva ad identificarla come se ne costituisse a tutti gli effetti il nome, ovvero lo pseudonimo.

dottrina è sostanzialmente concorde con questa posizione[19], anche se alcuni autori hanno manifestato perplessità in ordine al fatto che il soprannome virtuale fosse stato valorizzato dalla Corte non come alterazione soggettiva dell'agente, ma come strumento di determinazione del danno alla persona offesa, poiché il *nickname* in questione appariva talmente criptico da rendere impossibile un qualunque riferimento ad una persona reale[20].

L'ultimo caso affrontato dalla Cassazione in materia di furto d'identità e sostituzione di persona risale al 2014[21]: i giudici di legittimità hanno ritenuto configurabile il reato di cui all'art. 494 c.p. nella condotta di colui che aveva creato un profilo su un *Social Network* riportando un'immagine che riproduceva la persona offesa con una descrizione offensiva delle caratteristiche personali riferite al presunto titolare dell'*account* e si era servito di tale falsa identità per usufruire dei servizi del sito, comunicando in rete con altri iscritti[22].

Dato che il furto d'identità *online* è un fenomeno criminoso complesso che si articola in diverse fasi è però riduttivo limitarlo al delitto di sostituzione di persona previsto dall'art. 494 c.p., per cui occorre verificare la possibilità di applicare anche altre norme penali incriminatrici.

In relazione al fenomeno criminoso del *phishing* una prima sentenza del Tribunale di Milano[23] aveva stabilito che vi è concorso tra i reati di sostituzione di persona, truffa ed utilizzo indebito di carte di credito[24] nella condotta di colui che, mediante la tecnica cd. dello *smishing*, aveva illecitamente sottratto numeri di carte di credito, inviando a diversi soggetti SMS ingannevoli, nei quali gli ignari destinatari venivano invitati a nome della banca a contattare un numero telefonico, dove una voce registrata, fingendosi il *call center* dell'istituto emittente, richiedeva i dati delle suddette carte e poi, una volta acquisiti, li aveva utilizzati per effettuare degli acquisti all'insaputa dei titolari. Una parte della dottrina[25] ha ritenuto che il giudice di merito non abbia correttamente applicato la fattispecie della sostituzione di persona, dato che nel caso in esame si trattava di *Phishing Voip Attack*[26] e non vi era stato alcun contatto diretto con l'utente, in quanto la risposta avveniva tramite una casella vocale dove rispondeva una

---

[19] Così A. IEVOLELLA, *Nickname falso con cellulare vero: sostituzione di persona,* in *Dir. & giust.*, 2013, n. 10, p. 391 ss., p. 391 e G: STAMPANONI BASSI, *Osservazioni a Corte di Cassazione, sezione V, n. 18826, 28 novembre 2011,* in *Cass. pen.*, 2014, n. 1, p. 146 ss., p. 147.

[20] E. MENGONI, *Chattare con un nickname riconducibile ad altri (e comunicare il loro numero telefonico) integra il reato di sostituzione di persona.*, in *Cass. Pen.*, 2014, n. 1, p. 148 ss., p. 151.

[21] V. Cass. pen., sez. V, 23 aprile 2014, n. 25774.

[22] Per un commento cft. F. SANSOBRINO, *Creazione di un falso account, abusivo utilizzo dell'immagine di una terza persona e delitto di sostituzione di persona*, in *questa Rivista*, 30 settembre 2014.

[23] Trib. Milano, Ufficio G.I.P., 7 novembre 2007 in *Dir. Internet*, 2008, n. 3, p. 261.

[24] Fattispecie prevista all'epoca dei fatti prevista come reato dall'art. 12 l. 197/1991, in seguito sostituita dall'art. 55 del d.lgs. 21 novembre 2007, n. 231. Il Tribunale ha ritenuto che non vi fosse assorbimento di reati, in quanto la fattispecie di cui all'art. 55 d.lgs. cit., a differenza della truffa, non richiede che venga posto in essere alcun artificio.

[25] P. PERRI, *Lo smishing e il vishing,* cit., p. 267.

[26] In questo caso l'*e-mail* di *phishing* invita ad attivare una chiamata *Voice over IP*, ovvero tramite connessione *Internet* ad un *call center* apparentemente riconducibile ad un'istituzione reale.

voce elettronica registrata[27]. Secondo l'opinione dottrinale maggioritaria, invece, il Tribunale ha correttamente ravvisato l'esistenza del delitto di truffa *ex* art. 640 c.p.[28], data l'esistenza degli artifizi tipizzati dalla fattispecie e di tutti gli altri elementi costitutivi del delitto di truffa. Ma altra dottrina ha manifestato i propri dubbi per essere stato il reo ad effettuare la disposizione patrimoniale per conto del soggetto passivo[29], dato che la disposizione patrimoniale è un requisito implicito del delitto di truffa ed è espressivo della necessaria cooperazione da parte della vittima[30]. Per quanto riguarda l'applicabilità al caso in esame della fattispecie di indebito utilizzo di carte di credito, *nulla quaestio*: la condotta del *phisher* che inserisca i dati della carta di credito in un *form* in *Internet* è riconducibile a tale reato, che si consuma semplicemente con l'effettivo accesso ai servizi di prelievo di denaro contante o di acquisto di beni, senza necessità che vi sia la materiale disponibilità della carta[31].

In una successiva sentenza, sempre riguardante il fenomeno del *phishing*, il Tribunale di Milano[32] ha ravvisato in questa manifestazione criminosa il concorso tra le fattispecie di sostituzione di persona, truffa ed accesso abusivo ad un sistema informatico o telematico sanzionato dall'art. 615-*ter* c.p.: l'ultima fase dei *phishing attacks*, infatti, è diretta all'utilizzo delle informazioni raccolte, per accedere abusivamente ad aree informatiche riservate o a servizi *online*. L'art. 615-*ter* c.p. prevede, quale requisito tipico del fatto, la presenza delle misure di protezione del sistema, senza specificarne qualità, natura o efficacia. Quindi non vi è alcun dubbio sulla funzione protettiva delle abilitazioni necessarie per accedere a sistemi informatici, quali i nomi o i codici utente, i *pin*, le parole chiave o le password riservate[33].

Dato che le condotte di furto d'identità digitale hanno il loro fulcro nella sottrazione dei dati riservati degli utenti, un'ulteriore fattispecie che può assumere rilevanza è l'art. 615-*quater* c.p. Questo è un reato a forma libera, per cui non vi sono ostacoli a ritenere che la condotta sanzionata possa consistere nell'invio di *e-mail* o nell'installazione di *malware* con lo scopo di carpire i codici d'accesso[34]. Le *password* e i codici d'accesso, infatti, rientrano nel concetto di identità digitale, perché ontologicamente correlati all'identificazione del soggetto. Quindi, in alcuni casi, questa norma può assumere rilevanza, anche se non va dimenticato che i dati personali non sono affatto menzionati nell'art. 615-*quater* c.p. e che di conseguenza la loro specifica protezione non è direttamente oggetto del reato in questione.

---

[27] In questi termini P. PERRI, *Lo smishing e il vishing*, cit., p. 267.
[28] *Ibidem*.
[29] R. FLOR, *Phishing, identity theft,* cit., p. 903.
[30] V. C. PEDRAZZI, *Inganno ed errore nei delitti contro il patrimonio*, Milano, 1955, p. 59; G. FIANDACA – E. MUSCO, *Diritto penale, PS*, vol. II, tomo II, VI ed., Bologna, 2014, p.190.
[31] P. PERRI, Lo *smishing e il vishing*, cit., p. 269; R. FLOR, *Phishing, identity theft,* cit., p. 914.
[32] Trib. Milano, 7 ottobre 2011, in *Dir. pen proc.*, 2012, n.1, p. 55.
[33] R. FLOR, *Art. 615 ter c.p.: natura e funzioni delle misure di sicurezza, consumazione del reato e bene giuridico protetto*, in *Dir. pen proc.*, 2008, n.1, p. 106 ss., p. 107.
[34] V. Cass. pen., sez. II, 17 dicembre 2004, n. 5688, secondo cui anche i numeri telefonici ed i numeri seriali dei cellulari costituiscono codici di accesso a un sistema informatico o telematico, ai sensi della norma in esame, in quanto permettono di individuare l'utenza e l'apparato cui è abbinata.

3. Il nuovo terzo comma dell'art. 640-*ter* c.p. e il tentativo del legislatore di colmare il vuoto normativo.

L'art. 9 d.l. n. 93/2013 ha introdotto quale terzo comma dell'art. 640-*ter* c.p. una nuova circostanza aggravante ad effetto speciale del delitto di frode informatica, con la dichiarata intenzione di fornire maggiore tutela penale alle ipotesi di furto di identità digitale. Sulla natura di tale previsione vi è stata discussione in dottrina: se de un lato la sua collocazione sistematica fa propendere per la sua configurazione quale circostanza aggravante ad effetto speciale, vi sono altri elementi che invece rendono plausibile il suo inquadramento quale fattispecie autonoma[35]. Ciononostante quasi in modo unanime la dottrina ritiene che tale disposizione costituisca una circostanza aggravante della frode informatica[36].

In sede di conversione del decreto, il Parlamento ha radicalmente mutato la formulazione inizialmente prevista dal d.l. 93 cit. L'originaria locuzione «*se il fatto è commesso con sostituzione dell'identità digitale in danno di uno o più soggetti*» è stata infatti sostituita con l'inciso «*se il fatto è commesso con furto o indebito utilizzo dell'identità digitale*». La prima perplessità manifestata dalla dottrina riguarda proprio l'utilizzo improprio di tali termini: l'identità, infatti, è un'entità immateriale, pertanto non è certo definibile quale "cosa" che possa essere suscettibile di furto (*ex* art. 624 c.p.) o anche di venire materialmente "utilizzata"[37]. I primi commentatori hanno però accolto con favore la scelta di fondo del legislatore, in quanto la precedente formulazione era ritenuta troppo ambigua[38].

In ogni caso questa modifica ha sollevato un vivace dibattito in merito al significato, alla portata applicativa e ai limiti dell'espressione utilizzata. Il legislatore, infatti, non ha dato alcuna definizione di "identità digitale", con una scelta molto discutibile, perché oltre a creare difficoltà agli operatori del diritto pone anche seri problemi di legittimità costituzionale, dato che il precetto indeterminato è

---

[35] A sostegno di tale ultima tesi va rilevato che la frode informatica è una fattispecie posta a tutela del patrimonio, mentre il fenomeno del furto d'identità ha una connotazione più ampia, perché non si limita alle sole diminuzioni patrimoniali che da esso possono essere causate, quindi potrebbe trattarsi di una fattispecie autonoma volta alla tutela di beni giuridici diversi rispetto al patrimonio, quali l'identità digitale su *Internet*, la riservatezza informatica e l'affidabilità dei sistemi informatici e telematici. Un altro elemento che fa pensare che possa trattarsi di una nuova fattispecie autonoma è che non è previsto nel codice penale alcun articolo che punisca espressamente il furto d'identità digitale.

[36] V. F. MANTOVANI, *Diritto penale, PS, vol. II i delitti contro il patrimonio*, IV ed., Padova, 2016, p. 226.; M. MARGIOCCO, *Frode informatica*, in G. Finocchiaro – F. Delfini (a cura di), *Diritto dell'informatica*, Assago, 2014, p. 1107 ss., p. 1110; A. DI TULLIO D'ELISIS, *Frode informatica commessa con sostituzione dell'identità digitale: profili applicativi*, in Altalex 14 gennaio 2014.

[37] V. G. ZICCARDI, voce "*Furto d'identità*", in *Dig. disc. pen.*, tomo VI, aggior., Torino, 2001, p. 253 ss., p. 253; G. MALGIERI, *La nuova fattispecie di "indebito utilizzo d'identità digitale": un problema interpretativo*, in *Dir. pen. cont. – Riv. trim.*, 2/2015, p. 149 ss.

[38] Così L. PISTORELLI, *Relazione Ufficio del Massimario Cassazione*, n. III/01/2013 del 22 agosto 2013, p. 7.

potenzialmente lesivo del principio di tassatività in materia penale[39]. La nozione di identità digitale, infatti, non solo è priva di riscontri normativi, ma ha anche molteplici accezioni, ed in tal modo è arduo stabilire *a priori* ciò che è vietato e ciò che invece è consentito.

Una parte della dottrina ha cercato quindi di individuare i confini dell'identità digitale andando alla ricerca di definizioni espresse in sede extra-penale[40], tentativo che però si scontra col fatto che le diverse definizioni, quali ad esempio quella contenuta nell'art. 1, co. 1, del d.lgs. 82 del 2005 alla lett. u *quater*)[41], sono state create *ad hoc* per i provvedimenti nei quali sono inserite[42] e non sempre riescono a cogliere appieno la *ratio* sottesa all'introduzione di questa nuova disposizione nel sistema penale, specie se l'identità digitale è intesa come processo di identificazione informatica, perché in questo caso la nozione è limitata al momento della validazione in un sistema di un insieme di dati al fine di individuare all'interno di esso un soggetto utente legittimato a fruire di determinati servizi.

La novella legislativa contempla in ogni caso due diverse modalità di azione, aventi come oggetto l'identità digitale, quella del furto e quella del suo indebito utilizzo. La dottrina ha subito evidenziato che il legislatore non ha specificato in che cosa consistano queste due condotte[43]. Un significativo aiuto su che cosa debba intendersi per "furto d'identità digitale", concetto diverso rispetto al furto di cui all'art. 624 c.p. (dato che l'identità, come anticipato, non è una "cosa" suscettibile di spossessamento), arriva dai lavori parlamentari, in cui si legge che si debba fare riferimento all'art. 30-*bis* del d.lgs. n. 141 del 2010, che richiama il concetto di "impersonificazione"[44]. Tuttavia, ove

---

[39] F. MANTOVANI, *Diritto penale, PG*, cit., p. 61.

[40] Cft. A. DI TULLIO D'ELISIS, *Frode informatica*, cit.

[41] Essa definisce espressamente l'identità digitale come «*la rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità fissate nel decreto attuativo dell'articolo 64*». Tuttavia tale definizione è fornita espressamente ai fini del Codice dell'Amministrazione Digitale, che vede come destinatari solo lo Stato, le Regioni e le Province autonome, ed è circoscritta al fine di assicurare «*la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale*».

[42] Altre definizioni infatti sono: la prima quella introdotta ai soli fini della creazione e sviluppo del Sistema Pubblico per la gestione delle Identità Digitali di cittadini ed imprese, contenuta nell'art. 1 c. 1 lett. o) del decreto della Presidenza del Consiglio dei Ministri del 24 ottobre 2014, che tuttavia sembra far riferimento più ad una metodologia che consente l'identificazione informatica, piuttosto che ad un vero e proprio concetto di identità digitale; la seconda è quella contenuta nell'art. 3 del Reg. 910/2014/UE in materia di identificazione elettronica e servizi fiduciari, il quale però non fa riferimento al concetto di identità digitale, ma all'"identificazione elettronica" ed ai "dati di identificazione personale".

[43] G. MALGIERI, *La nuova fattispecie*, cit., p. 144.

[44] In tale articolo è infatti riportato che: «*ai fini del presente decreto legislativo*" (vale a dire per l'istituzione di un sistema di prevenzione delle frodi nel settore del credito al consumo) *"per furto d'identità si intende:*
a) l'impersonificazione totale: occultamento totale della propria identità mediante l'utilizzo indebito di dati relativi all'identità e al reddito di un altro soggetto. L'impersonificazione può riguardare l'utilizzo indebito di dati riferibili sia ad un soggetto in vita sia ad un soggetto deceduto;
b) l'impersonificazione parziale: occultamento parziale della propria identità mediante l'impiego, in forma combinata, di dati relativi alla propria persona e l'utilizzo indebito di dati relativi ad un altro soggetto, nell'ambito di quelli di cui alla lettera a)».

si ritenga che il furto d'identità coincida con l'impersonificazione, risulta complesso stabilire l'ambito applicativo dell'indebito "utilizzo" dell'identità digitale, perché anche colui che fa utilizzo di un'identità per fini diversi rispetto a quelli per cui era stato autorizzato apparentemente "impersonifica" un altro soggetto[45].

Problematiche persino maggiori presenta la seconda previsione dell'art. 640-*ter* co.3 c.p., ovvero "l'indebito utilizzo": un suggerimento sulla sua portata applicativa può derivare dall'art. 167 del d.lgs. n. 196/2003 cit., che sanziona l'illecito trattamento di dati personali, dato che la definizione di "trattamento" oggetto della previsione legale è molto ampia[46] e che in questa fattispecie è rilevante proprio l'abusivo utilizzo, rispetto alle finalità concordate, dei dati ottenuti con il pieno consenso dell'interessato. Tuttavia la dottrina evidenzia che non vi può essere corrispondenza univoca tra questa fattispecie e la nuova aggravante di cui al co. 3 art. 640-*ter* c.p. [47], dato che il concetto di "trattamento illecito" è diverso rispetto a quello di "indebito utilizzo": la nuova aggravante, infatti, punisce solo la sostituzione di persona digitale, tralasciando invece altre condotte, quali ad esempio il traffico non consentito di dati a fini commerciali o concorrenziali.

Secondo alcuni autori, quindi, l'unico modo per descrivere la condotta di "indebito utilizzo" e capire il suo rapporto col "furto d'identità digitale" è far riferimento alla rubrica dell'articolo «*sostituzione dell'identità digitale*»: l'effetto delle due fattispecie è identico, ma le modalità di esecuzione sono differenti, dato che nell'indebito "utilizzo" il possesso dei dati è lecito, ed è solo un determinato utilizzo non concordato che integra la violazione, mentre nel "furto" di dati la violazione del consenso vi è già nel momento della loro sottrazione[48].

Ulteriore perplessità della dottrina attiene al fatto che il "furto o indebito utilizzo di identità digitale" appare concepito dal nuovo co. 3 art. 640-*ter* c.p. soltanto come un'aggravante della frode informatica: pertanto né il furto di dati, né l'indebito utilizzo di identità digitale possono da soli integrare il reato di frode informatica, dato che serve almeno un trasferimento illecito da un patrimonio all'altro[49]. La tutela dal co. 3 art. 640-*ter* c.p. non può quindi operare per quei casi di furto o indebito utilizzo dell'identità digitale altrui che non sfocino in una diminuzione patrimoniale, ma che ad esempio comportino un'offesa all'onore o alla reputazione della vittima. Ad opinione della dottrina, che ha cercato di ampliare la portata della fattispecie in esame, nella definizione di "danno" può certamente rientrare anche il "lucro cessante", cioè il mancato guadagno

---

[45] V. G. MALGIERI, *La nuova fattispecie*, cit., p. 144; A. DI TULLIO D'ELISIS, *Frode informatica*, cit.

[46] La nuova definizione di trattamento, prevista dall'art. 4 del Regolamento UE 679 del 2016, direttamente applicabile dal 25.5.2018 è la seguente: «*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*».

[47] Così G. MALGIERI, *La nuova fattispecie*, cit., p. 149.

[48] G. MALGIERI, *La nuova fattispecie*, cit., p. 151.

[49] G. MALGIERI, *Il furto di identità digitale: una tutela patrimoniale della personalità*, in *La giustizia penale nella rete. Le nuove sfide della società dell'informazione nell'epoca di Internet*, a cura di R. Flor, D. Falcinelli, S. Marcolini, Milano, 2015, p. 37 ss., p. 40 s.

che la vittima subisce in seguito alla frode informatica commessa con furto d'identità digitale[50]. Tuttavia risulta evidente che quest'aggravante non è idonea a sopperire alla fattispecie codicistica di sostituzione di persona, che conserva comunque la sua importanza e consente di non lasciare vuoti di tutela in tutti i casi in cui la nuova disposizione può incontrare limiti applicativi.

La dottrina, dopo essersi a lungo interrogata se il *phishing* rientrasse nell'ambito applicativo della fattispecie tradizionale della truffa ovvero in quello della frode informatica[51], ha manifestato le sue perplessità relativamente al fatto che la nuova disposizione, nata proprio per punire questo fenomeno criminoso, sia stata inserita nella fattispecie della frode informatica, inidonea a ricomprendere al suo interno tale manifestazione criminosa, che per lo più integra la truffa comune *ex* art. 640 c.p.[52]. Questa scelta, quindi, paradossalmente rende difficile l'applicazione della nuova disposizione di cui al co. 3 art. 640-*ter* c.p. proprio nei casi che espressamente voleva sanzionare, anche se può certamente applicarsi ad altre diverse manifestazioni criminose: basti pensare al fenomeno del *pharming*[53], ove effettivamente si realizza un'alterazione del funzionamento del sistema informatico[54].

Il d.l. n. 93/2013, insieme all'introduzione del co. 3 art. 640-*ter* c.p., aveva provveduto anche ad inserire nell'art. 24-*bis* del d.lgs. n. 231/2001 il reato di frode informatica aggravato dalla sostituzione dell'identità digitale nel catalogo dei reati presupposto della responsabilità degli enti[55]. Ma questa disposizione, inspiegabilmente, in sede di conversione è stata eliminata. Tale scelta è sicuramente discutibile, poiché questa disposizione avrebbe consentito una maggior tutela dell'identità digitale, dato che nella maggior parte dei casi i soggetti che gestiscono i dati personali altrui sono degli enti, quali ad esempio gli istituti di credito.

---

[50] G. MALGIERI, *Il furto di identità digitale*, cit., p. 48. La giurisprudenza infatti ha mutuato dal campo civilistico il concetto di "danno patrimoniale", ricomprendendo in esso anche il "lucro cessante" e non solo il "danno emergente" v. Cass. pen., sez. II, 11 settembre 2013, n. 37170 e analogamente Cass. pen., sez. II, 16 settembre 2009, n. 40790. Secondo A. RICCI, *Il valore economico della reputazione nel mondo digitale. Prime considerazioni*, in *Contr. e impr.*, 2010, n. 6, p. 1297 ss., p. 1306 s. ciò consente di ipotizzare che nell'art. 640-*ter* co. 3 c.p. rientrino anche casi quali la sostituzione d'identità digitale commessa ai danni di un ente commerciale, che causa un danno all'immagine di quest'ultimo agli occhi del consumatore, oppure commessa nei confronti di un lavoratore, il quale subisce poi una ricaduta negativa nell'ambiente di lavoro o, infine, nei confronti di un persona nota, la cui lesione alla immagine pubblica finisca per arrecare un danno in termini di popolarità ed addirittura comporti una riduzione di introiti, con conseguente mancato guadagno.

[51] R. FLOR, *Phishing, identity theft e identity abuse*, cit., p. 910 ss. In giurisprudenza, infatti, è prevalsa la tesi della configurabilità della truffa: V. Trib. Milano, Ufficio G.I.P., 7 novembre 2007, cit.; Trib. Milano, Ufficio G.I.P., 29 ottobre 2008, n. 8542, cit.; In dottrina v. anche F. CAJANI, *Profili penali del phishing*, cit., p. 2296. Tale scelta però non è univoca, *a contrariis* v. anche Cass. pen., sez. V, 24 novembre 2003, n. 4576 e Cass. pen., sez. II, 24 febbraio 2011, n. 9891.

[52] F. CAJANI, *La tutela penale dell'identità digitale*, cit., p. 1097.

[53] V. *supra* par. 1.

[54] F. CAJANI, *La tutela penale dell'identità digitale*, cit., p. 1097.

[55] V. L. PISTORELLI, *Relazione Ufficio del Massimario Cassazione*, cit.

4. Brevi considerazioni conclusive.

L'identità digitale rappresenta un bene giuridico nuovo[56], distinto rispetto all'identità personale. Esso include due diverse accezioni: il diritto a non veder travisate le proprie opinioni e la propria essenza sul *web*, ed il diritto all'utilizzo esclusivo delle proprie generalità ed attributi nei sistemi informatici. Esso può essere ricompreso nel novero dei diritti della personalità, dato che il bene giuridico sottostante, ovvero l'identità nelle sue diverse manifestazioni anche virtuali, è correlato all'essenza della persona. Proprio per questo motivo si può agevolmente affermare che l'identità digitale è un bene giuridico primario e sicuramente meritevole di attenzione e di tutela penale.

Come si è visto, infatti, la discussione sulla tutela penale dell'identità digitale non può essere ricondotta alla sola tutela del patrimonio di fronte alle truffe e alle frodi informatiche, ma merita una più ampia riflessione, soprattutto perché le conseguenze psicologiche sofferte dalle vittime di furto d'identità virtuale sono pesanti. Oltre al danno patrimoniale o all'onore ed alla reputazione subìto, infatti, la persona offesa patisce anche una lesione della propria sfera più intima, della sua riservatezza e della sua qualificazione quale individuo libero di autodeterminarsi nel *cyberspace*.

Il diritto penale ha quindi un ruolo importante per la tutela dell'identità digitale rispetto ai comportamenti che ne costituiscono un'aggressione, poiché può garantirne la protezione con sanzioni proporzionate, adeguate e dissuasive, oltre a permettere all'Autorità una repressione più efficace del fenomeno criminoso globale del *Cybercrime*, di cui il furto d'identità digitale fa parte[57].

La legge penale vigente non è però adeguata a perseguire questa nuova manifestazione criminosa, poiché, come si è visto, non consente di punire tutte le diverse fasi e forme del furto d'identità. La scarsa consapevolezza del legislatore nei confronti della seria minaccia rappresentata da questo fenomeno criminoso è evidente: basti pensare che la proposta di legge diretta ad inserire nel codice penale una autonoma fattispecie per punire il furto d'identità digitale dopo essere rimasta abbandonata presso la Commissione giustizia per ben otto anni è oggi decaduta per il termine della legislatura[58].

Il legislatore italiano non è il solo a dimostrare scarsa attenzione verso la tutela del nuovo bene giuridico dell'identità digitale. Infatti in Europa continentale, nonostante diverse proposte legislative[59], non esiste ancora nessuno Stato che abbia inserito

---

[56] Sui nuovi beni giuridici nati con l'avvento dell'informatica v. L. PICOTTI, *Sistematica dei reati informatici*, cit., p. 70 e anche I. SALVADORI, *L'accesso abusivo ad un sistema informatico. Una fattispecie paradigmatica dei nuovi beni giuridici emergenti nel diritto penale dell'informatica*, in L. Picotti (a cura di), *Tutela penale della persona e nuove tecnologie, Quaderni per la riforma del codice penale*, Padova, 2013, p. 125 ss.

[57] Così L. PICOTTI, *Quale diritto penale nella dimensione globale del cyberspace?*, in Wenin R., Fornasari G. (a cura di), *Diritto penale e modernità: le nuove sfide fra terrorismo, sviluppo tecnologico e garanzie fondamentali*, Atti del convegno Trento, 2 e 3 ottobre 2015, Napoli, 2017, p. 309 ss., p. 313.

[58] La proposta di legge è accessibile a questo *link*.

[59] A titolo esemplificativo si riporta l'esistenza di una proposta di legge volta ad introdurre nel codice penale tedesco una nuova previsione legale per punire la cd. "ricettazione di dati" (o *Datenhelerei*) tramite l'inserimento del nuovo § 259a StGB, che dovrebbe consentire di punire anche la seconda fase del furto d'identità digitale, ovvero la vendita o

all'interno del proprio corpo codicistico delle nuove fattispecie incriminatrici *ad hoc* che consentano di punire tutte le diverse fasi e forme del furto d'identità digitale.

E non si può trascurare il fatto che il furto d'identità digitale è un fenomeno criminoso globale e transnazionale, per cui l'iniziativa dei singoli legislatori nazionali non appare sufficiente a garantire un'efficace protezione di questo nuovo bene giuridico. Nell'ambito dell'Unione Europea un ruolo chiave nel contrasto a questa nuova manifestazione criminosa può sicuramente essere svolto dal legislatore europeo, che potrebbe contrastare l'inerzia dei diversi legislatori nazionali con gli strumenti normativi a sua disposizione[60], in modo da adempiere finalmente a quelle raccomandazioni della Commissione europea, la quale già dieci anni fa ravvisava la necessità di adottare a livello europeo una fattispecie incriminatrice *ad hoc* con la funzione di tutelare l'identità digitale[61]. È quindi auspicabile un'azione più incisiva in materia di tutela penale dell'identità virtuale da parte del legislatore europeo, che con tale intervento potrebbe garantire una protezione adeguata ed effettiva a tale bene giuridico, mediante una direttiva *ad hoc* oppure nel quadro di un'armonizzazione più incisiva delle disposizioni penali dei diversi paesi europei in materia di lotta alla criminalità informatica, rispetto a quella assai circoscritta introdotta con la direttiva UE 40/2013[62].

cessione dei dati personali altrui illecitamente ottenuti.

[60] Dopo l'entrata in vigore del Trattato di Lisbona, che ha fatto venir meno la distinzione tra le competenze del "primo pilastro" e del "terzo pilastro" (in cui rientrava la cooperazione giudiziaria in materia penale), gli artt. da 82 a 86 del TFUE forniscono all'Unione Europea la competenza per armonizzare la legislazione penale dei diversi Paesi, sia nel campo del diritto penale sostanziale che in quello del diritto processuale. L'art. 83 TFUE in particolare prevede che l'Unione europea possa emanare norme minime relative alla definizione di reati e sanzioni in relazione a gravi crimini, anche in materia di *Cybercrime*. Cft. L. Picotti, *La nozione di "*criminalità informatica*" e la sua rilevanza per le competenze penali europee*, in *Riv. trim. dir. pen. econ.*, 2011, n. 4, p. 827 ss., *passim*.

[61] V. *Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cyber crime*, COM, 2007, accessibile a questo *link*.

[62] Tale direttiva prevede al *Considerando* 41 «*l'istituzione di efficaci misure contro il furto d'identità ed altri reati connessi all'identità*» ed al co. 5 art. 9 «*gli Stati membri adottano le misure necessarie ad assicurare che, qualora i reati di cui agli articoli 4 e 5 siano commessi abusando dei dati personali di un'altra persona allo scopo di guadagnare la fiducia di terzi, in tal modo arrecando un danno al legittimo proprietario dell'identità, ciò possa, conformemente al diritto nazionale, essere considerato una circostanza aggravante, purché tale circostanza non sia già contemplata da un altro reato punibile a norma del diritto nazionale*».