RASSEGNA ITALIANA DI CRIMINOLOGIA
ANNO VI N.1 2012

Facebook e rischio di pubblicare informazioni utili per reati d'identità

Facebook and the risk to publish useful information for id crimes

Andrea Cauduro

Parole chiave: Facebook • Furto d'identità • Privacy • Social network • Cybercrime

Riassunto
Negli ultimi anni i reati d'identità sono cresciuti molto, ma poco si è studiato come talvolta siano le vittime a diffondere involontariamente i propri dati personali. A questo riguardo i social network (Facebook in particolare) possono divenire una fonte di informazioni vastissima per criminali intenzionati a sottrarre/frodare identità altrui.
Questo articolo propone un modello di valutazione del rischio di reati d'identità che possono essere perpetrati utilizzando informazioni personali pubblicate su Facebook e rese visibili a chiunque abbia un account sul social network. Tale modello è stato poi impiegato per uno studio su 1000 utenti italiani di Facebook evidenziando come il 9,7% di questi condivida una serie di dati sensibili che li espone al furto/frode d'identità e quali siano le caratteristiche (età, genere, ecc.) di queste persone e potenziali vittime.

Keywords: Facebook • ID theft • Privacy • Social network • Cybercrime

Abstract
In the past few years identity crimes have strongly increased; however, only a few studies focused on how the same victims sometimes involuntarily spread their personal data. In this regard, social networks (and Facebook in particular) can become a huge source of information for criminals who aim at stealing/cheating identities.
This article proposes an evaluation model for the risk of identity crimes that can be perpetrated employing personal information published on Facebook and made visible to anyone with an account on the social network. This model has been then employed for a study on 1000 Italian Facebook users highlighting how 9,7% of them shares a series of personal data that exposes them to ID theft/fraud and the features (age, gender, etc.) of these persons and potential victims.

Per corrispondenza: Andrea Cauduro, Dipartimento di Scienze Giuridiche, Università degli Studi di Trento
e-mail • *andrea.cauduro@unitn.it*

ANDREA CAUDURO, Assegnista di ricerca in Sociologia giuridica, della devianza e del mutamento sociale, Dipartimento di Scienze Giuridiche, Università degli Studi di Trento

Facebook e rischio di pubblicare informazioni utili per reati d'identità

1. Reati d'identità: definizioni e ricerca in materia

1.1 *Furto e frode d'identità: definizioni*

Nella società dell'informazione identità reale e digitale si sovrappongono sempre di più portando a vulnerabilità legate all'uso, per scopi criminali, di dati personali reperiti online. Si pensi ad esempio al *phishing* con cui si possono sottrarre i codici di accesso al conto bancario di una persona e compiere movimenti di denaro non voluti (Elliott, 2010; Wall, 2007). Inoltre, i reati d'identità possono essere compiuti per facilitare l'ottenimento ad es. di contributi non dovuti e/o per sfuggire a sanzioni amministrative (si pensi ad esempio alla possibilità di utilizzare un'identità trafugata per ricevere delle sovvenzioni pubbliche o al contrario per sfuggire alla decurtazione dei punti sulla patente di guida). Infine, i crimini facilitati dalla sottrazione/alterazione d'identità possono avere scopi diversi dal guadagno truffaldino, ad esempio per mascherare altri reati: si pensi a casi di *cyberbullismo* o *stalking* perpetrati utilizzando le generalità di un terzo che sebbene all'oscuro di tutto, risulti insultare o perseguitare qualcuno su chat, forum o tramite programmi di messaggistica istantanea (es. Skype o Messenger) (Patchin & Hinduja, 2006; Smith, Mahdavi, Carvalho, Fisher, Russell, & Tippett, 2008; Zaller, 2011). In tutti i casi si nota come il reato d'identità sia un classico reato strumentale: cioè un comportamento criminale non fine a se stesso, ma strumento per la commissione di un altro illecito (es. frode o diffamazione).

In base alle caratteristiche dei crimini commessi, una parte degli studiosi definisce dunque *furto d'identità* (o impersonificazione[1]) l'uso illecito di un'identità realmente esistente. Al contrario, si parla di *frode d'identità*, quando viene creata un'identità parzialmente o completamente fittizia oppure quando viene contraffatta la propria (es. modificando i dati anagrafici) per scopi criminali[2] (Acoca, 2008, pp. 74-75; FPEG, 2007, p. 7).

Accanto a questa prima descrizione, alcuni altri ricercatori (soprattutto americani) preferiscono parlare semplicemente di furto d'identità e non di frode d'identità poiché ritengono che non sia l'identità ad essere frodata, bensì la vittima di un reato d'identità che si vede sottrarre denaro o altri beni a causa dell'abuso dei propri dati personali (Acoca, 2008; McNally & Newman, 2008, p. 2).

Altri studiosi mettono addirittura in discussione il concetto di furto d'identità ritenendo che al massimo si possa parlare di *abuso* d'identità poiché questa non possa essere in realtà rubata (Acoca, 2008, p. 74).

Infine, in questo dibattito sulle definizioni di reato d'identità, si sono inserite anche istituzioni come Europol (2006, p. 18) e le Nazioni Unite (UN IEG, 2007, pp. 4-5): questi e altri contributi definitori, seppur interessanti e utili, non saranno discussi in questa sede poiché non centrali per gli obiettivi di questo articolo.

1.2 *Ricerche sui reati d'identità in ambito internazionale, europeo ed italiano*

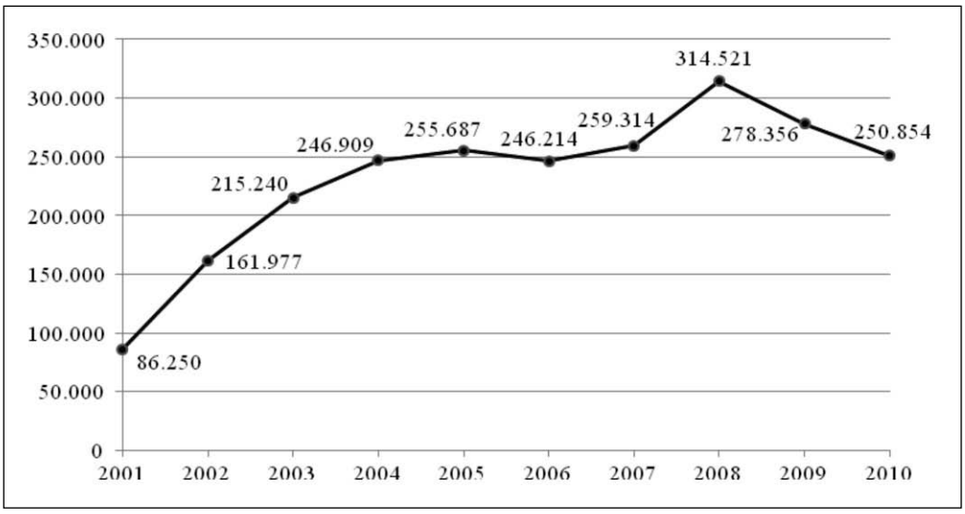
Sebbene i reati d'identità siano sempre esistiti, è indubbio che la diffusione di internet e delle nuove tecnologie abbia permesso una crescita esponenziale di simili comportamenti criminali. Quali sono dunque gli studi più autorevoli che si sono occupati di questa tipologia di reati? Cosa sappiamo su queste fattispecie e quali sono i limiti della conoscenza? Questo paragrafo propone una rassegna della letteratura internazionale, europea e nazionale in materia.

Una prima fonte è rappresentata dai rapporti annuali del *Consumer Sentinel Network* coordinato dalla *Federal Trade Commission* (FTC) americana che sin dal 2001 raccoglie dati sulle segnalazioni ricevute dalla *Federal Trade Commission* da parte di cittadini in merito ai furti d'identità subiti. L'ultimo rapporto disponibile (FTC, 2011, pp. 4-12) presenta un dato storico decennale per quanto riguarda le segnalazioni di furto d'identità negli Stati Uniti, come sintetizzato dal Graf. 1 sotto, che evidenzia come nell'arco di dieci anni le segnalazioni siano triplicate. È molto probabile che questo dato sia influenzato dalla maggior consapevolezza della popolazione riguardo ai reati d'identità che quindi è più propensa a denunciare eventuali abusi; tuttavia, è chiaro che le informazioni riportate sono un buon indicatore di come questi crimini siano in rapida ascesa.

1 Tale comportamento rientra nell'ipotesi di sostituzione di persona (art. 494 c.p.): *Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici, è punito, se il fatto non costituisce un altro delitto contro la fede pubblica, con la reclusione fino ad un anno.*

2 Fattispecie che può configurare il reato di false dichiarazioni sulla identità o su qualità personali proprie o di altri (art. 496 c.p.): *Chiunque, fuori dei casi indicati negli articoli precedenti, interrogato sulla identità, sullo stato o su altre qualità della propria o dell'altrui persona, fa mendaci dichiarazioni a un pubblico ufficiale, o a persona incaricata di un pubblico servizio, nell'esercizio delle funzioni o del servizio, è punito con la reclusione fino a un anno o con la multa fino a cinquecentosedici euro.*

Graf. 1 - Andamento del numero di segnalazioni per furto d'identità alla *Federal Trade Commission* degli Stati Uniti. 2001-2010



Fonte: elaborazione dell'autore di dati FTC, 2011: 5

Il rapporto della *Federal Trade Commission* non si limita a fornire il numero di furti d'identità segnalati, ma riporta anche le varie finalità di questo reato. Con riguardo al 2010, i casi presentano scopi di tipo frodatorio direttamente ai danni delle vittime, ma anche in danno di aziende e dello Stato per l'ottenimento di benefici indebiti a nome di ignari utenti. Al contrario, non sono chiaramente riconoscibili episodi di sottrazione d'identità a scopi di violenza (es. diffamazione online o bullismo). I dati del rapporto sono sintetizzati alla Tab. 1 sotto.

Tab. 1 - Percentuale delle finalità dei furti d'identità come riportato dalla *Federal Trade Commission* degli Stati Uniti. 2010 (N=250.854)

Finalità del furto d'identità	%
Illecito ottenimento di benefici statali (es. rimborsi fiscali)	19
Frode a carte di credito (es. apertura di nuovi conti)	15
Frode telefoniche (es. ottenimento di telefoni cellulari)	14
Frode in ambito lavorativo	11
Frode in ambito bancario (es. illecito trasferimento di fondi)	10
Frode in ambito creditizio (es. ottenimento di prestiti personali)	4
Altre finalità	22*

* Il totale non corrisponde al 100% poiché, come indicato (FTC, 2011, p. 11), il 12% dei furti d'identità segnalati aveva più di una finalità (es. frode bancaria e ai danni di carte di credito).

Fonte: elaborazione dell'autore di dati FTC, 2011: 11

Accanto alle finalità, il rapporto FTC (2011, p. 12) indica come il 72% delle vittime di furto d'identità abbia denunciato alla polizia il crimine. Questo dato è in netta crescita rispetto agli anni precedenti (2008-2009), in cui a fronte di un numero elevato di episodi, si è riscontrato un basso tasso di denuncia: nel 2008 solo il 28%, mentre nel 2009 la quota è salita al 62%. Infine, la ricerca segnala (2011, p. 13) come la maggior parte delle vittime (53%) abbia un'età inferiore ai 40 anni, con un picco tra i 20 e i 29 anni (24%), così come presentato dalla Tab. 3.

Tab. 3 - Età delle vittime di furto d'identità segnalato alla *Federal Trade Commission* degli Stati Uniti. 2010 (N=236.765)

Fasce d'età	%	∑%
≤ 19	8	8
20-29	24	32
30-39	21	53
40-49	19	72
50-59	15	87
60-69	8	95
≥ 70	5	100
Totale	100	-

Fonte: elaborazione dell'autore di dati FTC, 2011: 13

Accanto ai dati ufficiali relativi alle segnalazioni alla *Federal Trade Commission* e alle denunce alla polizia, una serie di studi sui furti d'identità ha cercato di comprenderne la diffusione, le finalità e i danni per le vittime e il sistema economico attraverso un approccio diverso: le indagini di vittimizzazione. A questo proposito e in merito all'età delle vittime, un'indagine di vittimizzazione con campionamento casuale condotta negli Stati Uniti dall'*Identity Theft Resource Center* (ITRC) nel 2009 ha evidenziato una situazione leggermente diversa da quella dipinta dai dati ufficiali, poiché si è rilevato come la maggior parte delle vittime (65% del totale) avesse meno di 49 anni, ma con uno spostamento anagrafico verso l'alto ed in particolare tra i 30 e i 49 anni, come si evince dalla Tab. 4 qui sotto.

Tab. 4 - Età delle vittime di furto d'identità negli USA come emerso dallo studio ITRC, 2009

Fasce d'età	%	∑%
≤ 18	3	3
18-29	14	17
30-39	26	43
40-49	22	65
50-60	26	91
≥ 61	9	100
Totale	100	-

Fonte: elaborazione dell'autore di dati ITRC, 2009: 6

Un altro importante esempio di indagine di vittimizzazione sui furti d'identità è la ricerca condotta da Synovate (2007, pp. 3-4), per la FTC. Lo studio ha stimato come il 3,7% della popolazione americana (pari a 8,3 milioni di persone) abbia subito un furto d'identità nel 2005 a scopo di frode. In particolare, il rapporto indica come l'1,5% della popolazione (3,3 milioni di persone) abbia subito tale reato con danni relativi ad assegni, conti bancari o utenze telefoniche; mentre l'1,4% (3,2 milioni di persone) abbia dichiarato di essere stato oggetto di un furto o abuso di una o più carte di credito in loro possesso e infine, lo 0,8% (1,8 milioni di persone) si è visto sottrarre l'identità con lo scopo di aprire nuove utenze, conti bancari, ecc. per commettere frodi celate dietro all'identità rubata.

Rispetto ai dati sulle segnalazioni, il valore aggiunto delle indagini di vittimizzazione risiede soprattutto nella mole di informazioni raccolte proprio sulle e dalle vittime di reato. In particolare, il rapporto Synovate del 2007 indica come le vittime nella maggior parte dei casi rilevino il furto d'identità in meno di una settimana, tuttavia una parte considerevole dei soggetti scopre gli abusi in tempi più lunghi talvolta superiori ai 6 mesi dall'episodio (Synovate, 2007, p. 23). Questo dato è confermato anche da ITRC che sottolinea come nel 47% dei casi l'abuso venga scoperto entro 3 mesi, anche se il 10% dei furti viene scoperto tra 4 e 6 mesi, mentre il 14% richiede tra 7 mesi e un anno e addirittura un 12% di episodi viene scoperto dopo 3 anni dal loro verificarsi (2009, pp. 17-18).

Un altro aspetto esplorato riguarda il rapporto vittima/autore. In base ai dati raccolti da Synovate nell'84% degli episodi l'autore è sconosciuto alle vittime e queste ultime nel 56% dei casi non sanno come le loro informazioni personali siano state ottenute dai ladri d'identità (2007, pp. 27-28). Tale ripartizione, tuttavia, non trova conferma nello studio dell'ITRC (ITRC, 2009, pp. 14-15) che al contrario indica come il 57% delle vittime dichiari di conoscere l'autore (es. parente, vicino di casa, collega, amico) mentre il 43% dichiari di non conoscere chi ha perpetrato il furto.

Accanto a questi aspetti, gli studi compiuti sulle vittime di furto d'identità permettono di comprendere altre sfaccettature connesse al reato ed in particolare le tempistiche per la risoluzione del problema e il danno economico subito. Per quanto riguarda la soluzione del problema i tempi possono variare da pochi giorni fino a 3 mesi o più (Synovate, 2007, pp. 25-26) o perfino alcuni anni come sottolinea ITRC (2009, p. 19). A quanto ammonta, invece, il danno economico "medio" patito dalle vittime? Synovate (2007, pp. 35-36) stima che il valore mediano delle perdite economiche sia di 500 dollari. Sullo stesso argomento, ITRC impiega dei criteri di stima diversi, soprattutto legati alla quantificazione delle ore perse per risolvere il problema, e dai dati proposti (2009, p. 19) emerge come le spese medie per "riparare" il danno arrecato a conti bancari esistenti ammontino a 739 dollari, mentre in caso di furto d'identità finalizzato all'apertura di nuovi conti, il costo medio salga a 951 dollari. Altro aspetto innovativo dell'analisi proposta da ITRC riguarda i danni patiti dalle aziende. Infatti, come visto, il fine ultimo del furto d'identità (es. frode, ottenimento di benefici indebiti) si ripercuote anche su soggetti terzi come banche, gestori di carte di credito, compagnie telefoniche. ITRC ha stimato per il 2008 una perdita media di 90.107 dollari per le aziende

che subiscono le conseguenze dei furti d'identità (2009, p. 22). Tali dati, tuttavia, possono variare notevolmente in base al tipo di azienda colpita e, come correttamente segnalato dagli autori, i dati impiegati per l'indagine di vittimizzazione non sono rappresentativi di tutta la popolazione di aziende degli USA, perciò la stima non può che essere approssimativa.

I dati sin qui visti per la realtà statunitense si riflettono anche in ambito europeo, sebbene il numero di ricerche sia molto più limitato. A questo riguardo, si segnalano alcuni rapporti condotti nel Regno Unito per la *National Fraud Authority* da parte di *CIFAS* un'organizzazione no-profit che si occupa di tutelare le vittime di furto d'identità e frode. In base ai dati più recenti (CIFAS, 2010, p. 3) nel 2010 sono stati rilevati 102.672 casi di reati d'identità, di cui oltre 89.000 casi di impersonificazione, con una crescita del 4,7% rispetto all'anno precedente. Inoltre, il rapporto evidenzia come anche le imprese siano spesso oggetto di attacchi e possano subire furti d'identità (2010, pp. 22-23).

Infine, cosa è stato fatto in Italia? Innanzi tutto va segnalato che nel nostro Paese l'interesse per la tematica si è sviluppato solo di recente. Tra le ricerche spiccano i rapporti curati dall'Osservatorio permanente sul furto d'identità (ADICONSUM, 2009; 2010) che hanno "scattato le prime fotografie" delle vittime di furto d'identità impiegando le tecniche delle indagini di vittimizzazione già sperimentate all'estero. Dai dati disponibili si deduce come il fenomeno sia diffuso anche in Italia, con conseguenze soprattutto per quanto concerne il settore finanziario con frodi legate a carte di credito o connesse ad acquisti effettuati online. A riguardo, l'ultimo rapporto (ADICONSUM, 2010), similmente a quanto prodotto dalle ricerche statunitensi suesposte, stima anche il danno economico patito dalle vittime ed in particolare evidenzia come il 41,8% abbia subito un danno fino a 500 euro, l'11,9% da 501 a 1000 euro, il 9,4% superiore a 1000 euro, mentre il 36,9% non sa quantificare. Come si può notare, tale distribuzione si pone sostanzialmente in linea con quanto espresso dalle ricerche condotte oltreoceano.

1.3 Facebook e furto d'identità: cosa si rischia

Come si è visto nel paragrafo precedente, la conoscenza delle dinamiche e delle tendenze dei reati d'identità non è ancora approfondita: gli studi sono spesso settoriali e non diffusi in tutto il mondo, le definizioni non sono univoche anche a causa dei repentini cambiamenti delle tecniche criminali, infine mancano quasi del tutto dati ufficiali forniti da statistiche di polizia o giudiziarie.

Accanto a questi limiti, che in parte si tenta di superare con indagini di vittimizzazione, alcune ricerche hanno studiato la realtà dei social network e come gli utenti di tali servizi possano (involontariamente) favorire i reati d'identità e l'abuso delle proprie informazioni personali (Acquisti & Gross, 2009; Brown, Howe, Ihbe, Prakash, & Borders, 2008; Gross & Acquisti, 2009; Krishnamurthy & Wills, 2010; Labitzke, Taranu, & Hartenstein, 2011; Lampe, Ellison, & Steinfeld, 2007).

Ma cosa succede, in concreto, a pubblicare dati personali su un social network come Facebook? Si può risalire da queste informazioni all'identità di una persona al fine di commettere un reato d'identità?

La risposta, purtroppo, è sì. E molto spesso sono proprio le stesse vittime a fornire (inconsapevolmente) i dati necessari ai criminali d'identità. Un primo rischio, infatti, riguarda la possibilità di calcolare il codice fiscale della vittima basandosi su nome, cognome, data e luogo di nascita, tutti dati che possono essere resi visibili dagli utenti di Facebook. Se poi sono condivisi altri dettagli come numero di cellulare, indirizzo, ecc. si intuisce agevolmente come possa essere grandemente facilitata una completa impersonificazione da parte di eventuali malintenzionati. Le ricerche indicano come una volta carpiti questi dati un criminale d'identità possa intraprendere diverse azioni partendo dalla creazione di documenti falsi che permettono di ottenere sconti, promozioni e/o beni presso negozi. Si pensi ad esempio alle promozioni di molti gestori telefonici che consentono di ottenere *smartphone*, computer, ecc. semplicemente sottoscrivendo un contratto. In caso di furto d'identità il contratto viene sottoscritto in un negozio, il criminale ottiene immediatamente ad es. un pc che poi rivende (senza ovviamente pagarlo onorando il contratto), ripetendo poi l'attività illecita con una nuova identità rubata, presso un altro rivenditore e così via. In questo caso, le vittime sono due: la persona cui viene sottratta l'identità e il gestore telefonico cui diventa difficilissimo se non impossibile recuperare i beni sottratti. Infatti, una volta che quest'ultimo cercherà di recuperarli si troverà a chiedere il pagamento a un soggetto ignaro e a sua volta frodato.

Tuttavia, come evidenziato dalla letteratura in materia, una volta sottratta l'identità altrui questa può essere impiegata anche ad esempio per fornire generalità appartenenti a un soggetto terzo così da sfuggire a sanzioni. Si pensi al caso in cui sia contestata un'infrazione per eccesso di velocità e guida in stato d'ebbrezza. Se il guidatore avesse con sé dei documenti falsi ottenuti rubando dati appartenenti a una persona realmente esistente, potrebbero scattare delle conseguenze per un soggetto estraneo alla vicenda. Similmente, invece di tentare di evitare una sanzione, sempre impiegando dati falsi può essere facilitata un'attività illecita per ottenere sussidi, contributi statali e così via a nome di una persona che ha formalmente i requisiti necessari (es. età, disabilità).

Inoltre, anche se l'area è poco esplorata dalla ricerca, non si devono dimenticare le ipotesi in cui dati identificativi siano sottratti per compiere reati non appropriativi, come gli atti persecutori (*stalking*). Si pensi ad esempio al caso di una donna che cambi indirizzo, numero di telefono, ecc. per sfuggire allo *stalking* dell'ex marito. Questi potrebbe accedere a un social network, sottrarre dati personali di un'amica dell'ex coniuge e, spacciandosi per quest'ultima, carpire il nuovo indirizzo e ricominciare le molestie.

Infine, sempre riguardo a furti d'identità finalizzati a reati non appropriativi, non vanno trascurati minacce, episodi di bullismo e cyberbullismo, ma anche ad esempio casi di pedopornografia online che possono essere celati dietro l'identità fasulla rendendo da un lato difficile l'identificazione del reale colpevole e dall'altro indirizzando i sospetti sulle vittime del furto d'identità che si vedrebbero addossare responsabilità non proprie.

1.4 Furto d'identità e Facebook: obiettivi della ricerca

Sulla scia di quanto detto sopra, nei prossimi paragrafi si presentano i risultati di uno studio sul più famoso e diffuso social network del mondo: Facebook, che a ottobre del 2011 conta oltre 800 milioni di account attivi sparsi in tutti i continenti[3] di cui oltre 20 milioni solo in Italia[4].

La ricerca, in particolare, si pone questi due obiettivi:

a) elaborare un modello per valutare se e quanto un utente è a rischio di furto d'identità in base al numero e al tipo di informazioni personali che rende visibili a chiunque su Facebook;
b) applicare tale modello ad un campione di utenti italiani di Facebook evidenziando il numero di soggetti a rischio e le loro caratteristiche.

2. Metodologia

2.1 Individuazione delle variabili e modalità di raccolta dei dati

Molti profili di Facebook riguardano personaggi di serie televisive (es. i protagonisti della serie *Lost*) che quindi non sono realmente esistenti, oppure descrivono locali pubblici, luoghi turistici, ecc., infine non mancano profili di animali e di persone completamente inventate. Tuttavia, com'è noto, la maggior parte degli account appartiene a individui realmente esistenti. Come capire, dunque, se un utente (va da sé realmente esistente) rischia un reato d'identità a causa delle informazioni personali pubblicate su Facebook? La metodologia qui sotto descritta è stata impiegata per la presente ricerca partendo da alcune considerazioni e alcuni vincoli tecnici relativi al più famoso social network del mondo.

Innanzi tutto, va rilevato come la composizione della popolazione di Facebook (universo di riferimento) sia in gran parte sconosciuta: sappiamo a grandi linee le nazionalità degli utenti[5], ma non sappiamo se questi siano più maschi o femmine, più i ventenni o i sessantenni (anche se è ragionevole pensarlo) e così via. Inoltre, anche se possedessimo tali informazioni, non si potrebbe comunque avere la certezza che i dati inseriti siano completamente affidabili (es. una data di nascita e un luogo inventati, ecc.). La conseguenza di questa scarsità di informazioni sulla popolazione di riferimento, rende impossibile condurre degli studi su un campione rappresentativo di essa. Come fare dunque a concentrare la ricerca sugli utenti italiani e capire se sono prudenti/imprudenti nel diffondere i propri dati personali su questo social network?

Per rispondere a tale quesito si è partiti dalla considerazione che buona parte dei profili presenti su Facebook appartengono a persone reali che condividono informazioni altrettanto reali. Dopodiché, per circoscrivere la ricerca il più possibile, si sono individuati i 100 cognomi più diffusi in Italia[6] per aumentare al massimo la probabilità di trovare persone nate nel nostro Paese. Infine, si è creato un profilo fittizio (Zachary Robinson), senza alcun legame di amicizia con altri utenti di Facebook[7] e si è impiegata l'applicazione per Facebook *advanced search beta 2.2*[8] per selezionare 10 account per ogni cognome tra i 100 più diffusi nel nostro Paese. Ciò ha permesso, dunque, di selezionare 1000 utenti di Facebook con una probabilità molto alta di essere italiani. La ricerca è stata poi raffinata manualmente al fine di migliorare al massimo l'attendibilità di questi risultati scartando alcuni profili di "persone pubbliche" o di persone nate e cresciute all'estero, ma con nome e cognome italiani o profili da cui non si potesse ricavare un nome e cognome completi (come nel caso di persone con cognome intero e nome alterato da un diminutivo come "Ary", "Danny", ecc.).

Riguardo ad *advanced search beta 2.2*, va sottolineato che al momento della raccolta dati l'applicazione consentiva la ricerca solo tra i profili "*most detailed*", "*youngest*" e "*oldest*". Ai fini dell'articolo si è scelto di utilizzare il criterio "*most detailed*" per ottenere account non influenzati dall'età degli utenti e soprattutto poiché tale impostazione ha permesso di reperire persone potenzialmente più a rischio che condividono un numero di informazioni più elevato rispetto ad altri[9].

Facebook raccoglie molte informazioni personali sui suoi utenti: genere, età, residenza, numero di cellulare, gusti musicali, cinematografici, sportivi e così via. Tutte queste componenti formano il profilo di un utente e possono essere rese visibili a tutti gli utilizzatori del social network, oppure solo ad alcuni selezionati dal titolare del profilo, o a nessuno. Ovviamente non tutte le informazioni sono strategiche per un eventuale reato d'identità (es. preferenze musicali, film preferiti) e quindi per questa ricerca si sono individuati quegli elementi che possono essere impiegati per un reato d'identità. Tali componenti sono poi state operazionalizzate impiegando le modalità già presenti in Facebook o rielaborandone alcune e infine inserite in una matrice di dati, i cui risultati sono esposti di seguito.

Per alcune variabili le modalità raccolte sono state sì/no al fine di rilevare se tale informazione fosse visibile a tutti o meno (es. università, scuola superiore, orientamento religioso). Per altre invece si è proceduto a una semplificazione dei dati imputabili: è questo il caso del luogo di nascita/residenza. Infatti, nonostante gli utenti abbiano pubblicato la

3 Dati pubblicati da Facebook aggiornati a ottobre 2011 e reperibili al sito internet: www.facebook.com/press/info.php?statistics.

4 Dati pubblicati da Socialbakers aggiornati a ottobre 2011 e reperibili al sito internet: www.socialbakers.com/facebook-statistics.

5 Anche in questo caso i dati sono pubblicati da Socialbakers (aggiornati a ottobre 2011) e reperibili al sito internet: www.socialbakers.com/facebook-statistics.

6 Grazie al sito www.cognomix.it.

7 Soprattutto nessun legame con il profilo dell'autore, al fine di evitare possibili influenze nelle ricerche degli utenti, poiché Facebook indirizza la ricerca di persone in base a possibili amici comuni, parenti, eccetera.

8 L'applicazione, che richiede l'autorizzazione a usare il proprio profilo Facebook, è disponibile al sito internet: http://theprofileengine.com.

9 Va qui sottolineato che nella fase di stesura di questo articolo è stata rilasciata la versione definitiva di *advanced search* reperibile al sito http://profileengine.com. Tale versione del programma presenta alcune differenze rispetto alla versione beta impiegata per la raccolta dei dati qui impiegati.

città precisa di nascita/residenza (es. Avigliano, Valdobbiadene), le informazioni sono state registrate in base alla provincia in cui questa si trova al fine di non avere dati troppo dispersi. Similmente, nonostante Facebook consenta di conoscere giorno, mese e anno di nascita di un utente, si è raccolto solo l'anno di nascita.

Tutti i dettagli sulle variabili e le modalità raccolte sono sintetizzati dalla Tab. 5 qui sotto.

Tab. 5 - Variabili e modalità raccolte per identificare i profili di rischio degli utenti di Facebook

Variabile raccolta	Modalità
Foto	1 = Identificativa 2 = Non identificativa 3 = Nessuna foto
Genere	1 = Maschio 2 = Femmina
Università	1 = Sì 2 = No
Superiori	1 = Sì 2 = No
Luogo di residenza	1-110 = Province italiane 111 = Estero
Luogo di nascita	1-110 = Province italiane 111 = Estero
Lingue straniere parlate	1 = 1 2 = 2 3 = 3 4 = 4 o più
Data di nascita	Anno di nascita
Orientamento religioso	1 = Sì 2 = No
Orientamento politico	1 = Sì 2 = No
Orientamento sessuale	1 = Uomini 2 = Donne 3 = Uomini e donne
Situazione sentimentale	1 = Single 2 = Impegnato/a 3 = Fidanzato/a ufficialmente 4 = Sposato/a 5 = In una relazione complicata 6 = In una relazione aperta 7 = Vedovo/a 8 = Separato/a 9 = Divorziato/a
Messaggistica istantanea	1 = Sì 2 = No
Cellulare	1 = Sì 2 = No
Indirizzo postale	1 = Sì 2 = No

Fonte: elaborazione dell'autore

2.2 *Elaborazione di un metodo per la valutazione dei profili a rischio*

Dopo aver identificato ed operazionalizzato le variabili da raccogliere ai fini della ricerca, si è elaborato un modello che è stato utilizzato per individuare quanti utenti di Facebook con un'alta probabilità di essere italiani presentino un profilo a rischio per un reato d'identità.

Punto di partenza per la valutazione è la considerazione che Facebook può rappresentare una fonte di informazioni personali molto ricca soprattutto per impersonificazioni vere e proprie di soggetti terzi. Infatti, un'identità completamente fittizia può essere agevolmente creata senza l'ausilio di alcuna fonte di dati personali altrui, essendo sufficiente una certa dose di fantasia e di verosimiglianza di tale identità con persone (potenzialmente) esistenti: ad esempio sarebbe evidentemente non credibile un'identità "Alessandro Rossetti nato a Mantova il 13 ottobre 1873"; al contrario il profilo di un ipotetico "Alessandro Rossetti nato a Milano il 22 luglio 1968" avrebbe più possibilità di successo.

Il modello di valutazione della sicurezza di un profilo si basa, dunque, innanzi tutto su *quante* tra le seguenti sette informazioni personali raccolte da Facebook si aggiungono a nome e cognome (obbligatori per la creazione di un profilo) e siano visibili a tutti gli utenti del social network: 1) genere, 2) luogo di residenza, 3) luogo di nascita, 4) data di nascita, 5) indirizzo, 6) numero di cellulare, 7) contatto di messaggistica istantanea. Maggiore è il numero di dati visibili, maggiore è il rischio che quel profilo possa divenire appetibile per un eventuale reato d'identità.

Accanto al criterio quantitativo è stato impiegato, però, anche un approccio qualitativo. Infatti, il rischio di un reato d'identità non è dato solo da *quante* informazioni possono essere carpite, ma anche da *quali* dati sensibili sono accessibili liberamente a eventuali malintenzionati. Per questo motivo, nel modello proposto lo spartiacque che divide i profili sicuri da quelli insicuri è dato sia dal numero di informazioni, sia dalla visibilità dei dati necessari per ricavare *almeno* il codice fiscale di una persona (cioè nome e cognome, genere, data di nascita, luogo di nascita). Infatti, si pensi ad esempio a due soggetti che condividono lo stesso numero di dettagli. Il primo pubblica: 1) nome, 2) cognome, 3) genere, 4) contatto di messaggistica istantanea e 5) luogo di residenza; il secondo: 1) nome, 2) cognome, 3) genere, 4) data di nascita e 5) luogo di nascita. È chiaro come sia proprio la qualità delle informazioni a rendere i due profili diversi e soprattutto il secondo maggiormente appetibile per eventuali reati d'identità. Sulla scorta di queste considerazioni, ai fini di questa ricerca, si sono identificati quattro gradi di sicurezza per i profili esaminati e riportati di seguito in base al numero/qualità di informazioni che si aggiungono al nome e cognome che sono i punti minimi da indicare quando si crea un profilo di Facebook.

1. *Molto sicuro*: in questo caso è condiviso solo il genere dell'utente. Ciò è dovuto al fatto che questa informazione è obbligatoriamente visibile a tutti per le impostazioni di Facebook relative alle persone fisiche.
2. *Sicuro*: in questo caso il numero di informazioni è più alto (al massimo tre), tra luogo di residenza; luogo di nascita; data di nascita; indirizzo; numero di cellulare; contatto di messaggistica istantanea. In ogni caso, tuttavia, il numero e la combinazione dei dettagli visibili non sono idonei a carpire un codice fiscale.
3. *Insicuro*: in questo caso le informazioni visibili sono da tre a quattro e sono sufficienti ad ottenere il codice fiscale.
4. *Molto insicuro*: infine in questo caso il numero di informazioni visibili va da cinque a sette permettendo sia di ottenere il codice fiscale sia altri dettagli personali importanti (es. numero di cellulare e/o indirizzo).

La suddivisione nelle quattro categorie di sicurezza dei profili identificati è sintetizzati sotto alla Tab. 6.

Tab. 6 - Sicurezza dei profili degli utenti di Facebook basata sul numero e la tipologia delle informazioni visibili a tutti gli utenti del social network

Sicurezza del profilo	Informazioni pubblicate
Molto sicuro	Genere
Sicuro	Genere *e informazioni riguardanti* ***al massimo due*** *tra:* a) luogo di residenza; b) luogo di nascita; c) indirizzo; d) numero di cellulare; e) contatto di messaggistica istantanea *oppure informazioni riguardanti* ***al massimo due*** *tra:* a) luogo di residenza; b) data di nascita; c) indirizzo; d) numero di cellulare; e) contatto di messaggistica istantanea
Insicuro	Genere Luogo di nascita Data di nascita *ed eventualmente informazioni riguardanti anche*: luogo di residenza
Molto insicuro	Genere Luogo di residenza Luogo di nascita Data di nascita *e informazioni riguardanti* ***uno o più*** *tra:* a) indirizzo; b) numero di cellulare; c) contatto di messaggistica istantanea

Fonte: elaborazione dell'autore

3. Descrizione del campione individuato

Come accennato poc'anzi, dopo aver elaborato un metodo per valutare il rischio di furto d'identità su Facebook, si è applicato tale modello a un campione di 1000 utenti italiani. I risultati sono esposti di seguito.

Un primo dato che emerge dal campione rilevato è la prevalenza di utenti maschi: 76,9% di uomini contro 23,1% di donne. Come accennato nel paragrafo precedente, il motore di ricerca impiegato ha selezionato gli utenti che pubblicano più dettagli e questo fa dedurre che tendenzialmente siano proprio gli uomini a condividere un numero maggiore di informazioni. Tuttavia, tale risultato va letto anche in un'ottica qualitativa: i soggetti selezionati condividono ad esempio moltissime informazioni su gusti musicali, squadre di calcio o atleti preferiti, ma questo tipo di dettagli non espone al rischio di reato d'identità; mentre al contrario pubblicare poche informazioni inerenti a luogo e data di nascita, residenza, numero di cellulare può aumentare l'insicurezza.

Accanto al genere, si sono catalogate le foto inserite dagli utenti dividendole in "identificative", cioè in cui è possibile riconoscere la persona, "non identificative", in cui ciò non è possibile (es. foto di un paesaggio) e infine "nessuna foto". Il primo rilievo riguarda il fatto che il 99,8% del campione ha una foto. Più in dettaglio emerge come il 53,7% dei maschi abbia una foto identificativa, mentre tra le femmine si sale al 61%, come si può vedere sotto alla Tab. 7.

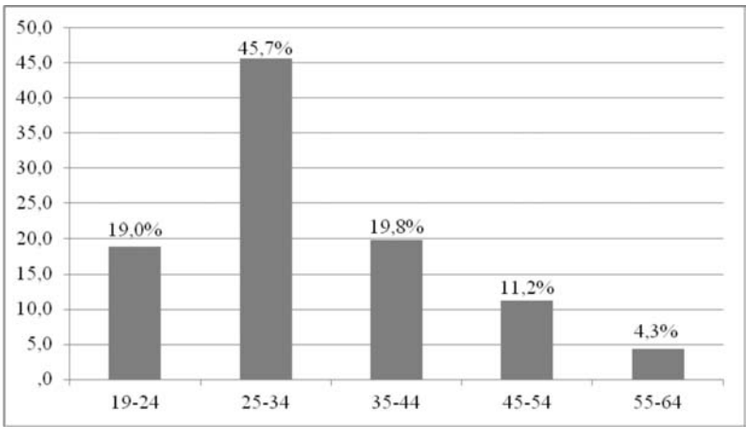
Tab. 7 - Percentuale del genere dell'utente per tipo di foto pubblicata (Nfemmine=231; Nmaschi=769)

	Foto			
Genere	**Identificativa**	**Non identificativa**	**Nessuna foto**	**Totale**
Maschio	53,7%	46,2%	0,1%	100,0%
Femmina	61,0%	38,5%	0,4%	100,0%

Fonte: elaborazione dell'autore

Per quanto riguarda l'età, l'11,6% del campione ha fornito la data di nascita e, come si può osservare alla Graf. 2, la fascia d'età più rappresentata è quella che va dai 25 ai 34 anni (45,7%), mentre si osserva l'assenza di minorenni e di persone con 65 anni o più.

Graf. 2 - Distribuzione delle fasce d'età degli utenti esaminati (N=116)



Fonte: elaborazione dell'autore

Continuando la panoramica, emerge come il 58,1% dei soggetti indichi il luogo di nascita e a questo riguardo, ai primi tre posti per diffusione si rilevano le province di Roma (11,4%), Milano (7,6%) e Napoli (7,4%). Per quanto riguarda, invece, il luogo di residenza il 54,3% del campione fornisce dei dettagli e anche in questo caso la provincia di residenza più diffusa risulta essere quella di Roma (13,1%), seguita da un paese straniero (10,5%) e dalla provincia di Milano (8,3%).

Per quanto riguarda l'istruzione Facebook consente di inserire informazioni solo riguardo a due istituzioni scolastiche: le scuole superiori e l'università. Tuttavia, qui sorge un problema interpretativo, poiché molti utenti non indicano nulla rispetto alla loro istruzione. L'assenza di tali dettagli in un profilo può essere dovuta al fatto che o un utente non ha frequentato la scuola superiore/università oppure (molto più probabilmente) perché ha semplicemente scelto di non indicare nulla. Per quanto concerne il campione esaminato, il 65,1% degli utenti non fornisce dettagli, il 23,8% dichiara di aver frequentato l'università e l'11,1% di essersi fermato alle scuole superiori.

Infine, riguardo alla situazione sentimentale, il 22,5% del totale indica il proprio status e tra questi, vi è una prevalenza di soggetti con una relazione sentimentale (impegnati, fidanzati, sposati, ecc.) come sintetizzato dalla Tab. 8.

Tab. 8 - Situazione sentimentale degli utenti esaminati (N=225)

Situazione sentimentale	%
Single	35,1
Impegnato/a	17,3
Fidanzato/a ufficialmente	16,0
Sposato/a	27,6
In una relazione complicata	1,3
In una relazione aperta	0,9
Vedovo/a	0,4
Separato/a	0,9
Divorziato/a	0,4
Totale	100,0

Fonte: elaborazione dell'autore

4. Risultati della ricerca

4.1 *Analisi della sicurezza dei profili: cosa condivide chi è a rischio?*

In base al modello proposto è possibile rilevare (Tab. 9) come la grande maggioranza del campione (90,3%) presenti un profilo sicuro o molto sicuro, mentre il 9,7% degli utenti condivida informazioni che rendono il loro profilo insicuro o molto insicuro. Sebbene questo dato possa apparire "confortante" e sebbene il campione analizzato non possa essere considerato pienamente rappresentativo degli italiani su Facebook, va comunque detto che se una percentuale vicina al 10% (ma in fondo anche molto inferiore) degli utenti italiani proteggesse in modo inefficace i propri dati personali sul noto social network, saremmo di fronte a svariate migliaia di persone che forniscono inconsapevolmente informazioni sensibili online con il rischio di esporsi a reati d'identità[10]. È per questo motivo, dunque, che di seguito ci si focalizza sull'analisi dei profili insicuri e molto insicuri al fine di rispondere alle domande: chi sono i soggetti a rischio e cosa condividono in concreto?

Nell'analisi proposta, va evidenziato come i risultati siano presentati in forma aggregata (profili "Insicuro" e "Molto insicuro" assieme), poiché entrambe le categorie fanno riferimento a persone che si pongono in una situazione di rischio rispetto a un reato d'identità. Inoltre, va rimarcato come i soggetti con un profilo "Molto insicuro" siano solo il 2,1% del campione (pari a 21 unità) di conseguenza qualsiasi analisi statistica condotta su un sottoinsieme così piccolo sarebbe azzardata poiché la variazione di una singola unità di valore assoluto porterebbe a scostamenti percentuali ingenti.

Per quanto riguarda il genere, il 77,3% dei profili a rischio appartiene a un maschio, mentre il 22,7% a una femmina rimanendo sostanzialmente in linea con la distribuzione tra i generi per i soggetti sicuri: 76,9% uomini e 23,1% donne. Per quanto riguarda la distribuzione anagrafica, la Tab. 10 evidenzia come la fascia d'età maggiormente rappresentata sia quella tra i 25 e 34 anni (45,4%) seguita dai ragazzi tra i 19 e i 24 anni (20,6%). Tale dato è probabilmente influenzato dalla grande popolarità di Facebook tra i giovani e la (probabile) minor diffusione tra le persone più mature, per cui è verosimile che anche le persone a rischio si concentrino nelle fasce d'età più basse. Inoltre, si nota una coincidenza con gli studi compiuti oltreoceano che individuano proprio in queste fasce d'età la concentrazione di reati d'identità subiti.

Per quanto riguarda le immagini associate al profilo (come si evince dalla Tab. 12 sotto), si rileva come sia i maschi sia le femmine con profili a rischio tendano a pubblicare foto identificative con una frequenza maggiore rispetto ai loro pari con profili più sicuri. In particolare, foto identificative sono pubblicate dal 64% dei maschi e dal 72,7% delle femmine "insicuri", mentre queste percentuali scendono al 52,6% dei maschi e al 59,8% delle femmine "sicuri".

Tab. 9 - Distribuzione della sicurezza dei profili Facebook per il campione analizzato. (N=1000)

Sicurezza del profilo	%	∑%
Molto sicuro	34,0	34,0
Sicuro	56,3	90,3
Insicuro	7,6	97,9
Molto insicuro	2,1	100,0
Totale	**100,0**	**-**

Fonte: elaborazione dell'autore

Tab. 10 - Percentuale dell'età degli utenti dei profili "Insicuro" e "Molto insicuro" (N=97)

Fascia d'età	%
19-24	20,6
25-34	45,4
35-44	18,6
45-54	11,3
55-64	4,1
Totale	**100,0**

Fonte: elaborazione dell'autore

10 Come accennato sopra si stima che gli utenti italiani di Facebook siano quasi 20 milioni.

Tab. 12 - Percentuale del genere dell'utente per tipo di foto pubblicata (profili "Insicuro" e "Molto insicuro", N=97) (profili "Sicuro" e "Molto sicuro", N=903)

Tipo di foto	Profilo	M	F
Identificativa	*Insicuro/molto insicuro*	64,0%	72,7%
	Sicuro/molto sicuro	52,6%	59,8%
Non identificativa	*Insicuro/molto insicuro*	36,0%	27,3%
	Sicuro/molto sicuro	47,3%	39,7%
Nessuna foto	*Insicuro/molto insicuro*	-	-
	Sicuro/molto sicuro	0,1%	0,5%

Fonte: elaborazione dell'autore

Tenendo a mente quanto detto in merito al problema interpretativo sulle persone che nulla dicono in merito alla propria istruzione, si nota come tra i soggetti a rischio il 38,1% dichiari di avere frequentato l'università, il 23,7% la scuola superiore e infine il 38,1% non fornisca informazioni. Per quanto riguarda invece la dislocazione geografica, le prime tre province di nascita sono Roma (12,4%), Milano (11,3%) e Napoli (8,2%), mentre in merito alla residenza la prima provincia è quella di Milano (13,1%) seguita da Roma (10,7%) e Napoli (6,0%).

Come anticipato, alcuni utenti oltre a fornire dati sufficienti per il calcolo del loro codice fiscale, pubblicano anche dettagli personali che rendono il loro account di Facebook particolarmente appetibile ad eventuali malintenzionati. In dettaglio, tra i profili a rischio del campione, l'11,3% indica anche il proprio indirizzo postale, il 14,4% un contatto di messaggistica istantanea (es. Skype, Messenger) e un altro 11,3% il numero di cellulare. Nel 5,2% dei casi, tutte queste informazioni sono pubblicate contemporaneamente.

Infine, accanto a queste variabili particolarmente sensibili, il 41,2% degli individui indica quale sia la propria religione, il 36,1% il proprio orientamento politico e il 68,0% le proprie preferenze sessuali. Questi dettagli sono poco utili per i crimini d'identità, tuttavia evidenziano come i soggetti a rischio siano propensi a "mettersi a nudo", anche se non è possibile chiarire se questa grande visibilità sia dovuta a una scelta consapevole, a sviste nella gestione della propria privacy, o alla mancata conoscenza degli strumenti di Facebook necessari a tutelare le proprie informazioni personali.

Conclusioni

Alla luce di quanto emerso dallo studio della letteratura e dall'analisi dei dati raccolti, è chiaro come la tutela dell'identità sia sempre più una priorità nell'odierna società, poiché i dati sensibili che identificano una persona possono trasformarsi in "merce" appetibile per criminali (anche organizzati) che abbiano l'intento di frodare delle persone, ma anche di ottenere ingiusti benefici se non addirittura di sottrarsi a sanzioni o commettere altri reati sfruttando le generalità altrui. A questo proposito, per sottolineare una volta di più come i furti d'identità possano avere conseguenze economiche ingenti e colpire un vasto numero di persone, vale la pena ricordare il caso di Rogelio Hackett Junior che nel 2009 è stato arrestato negli Stati Uniti per frode dopo aver sottratto ed indebitamente utilizzato 675.000 carte di credito per un danno di oltre 36 milioni di dollari (Zetter, 2011).

Come si è visto, tuttavia, i reati d'identità possono essere favoriti involontariamente proprio da chi subisce tali atti criminali e in questo settore Facebook e gli altri social network possono giocare un ruolo di primo piano. Per questo motivo sono quanto mai necessari altri studi che mirino ad investigare le possibili connessioni tra il mondo del social networking, la tutela dei dati personali e i reati d'identità. Infatti, l'immagine che abbiamo oggi sui reati d'identità rimane sfocata: pochi i dati, incerte le interpretazioni. Indubbiamente, le indagini di vittimizzazione impiegate per condurre alcune tra le ricerche più rilevanti hanno permesso di ottenere un quadro più preciso del fenomeno, ma molte domande rimangono ancora aperte soprattutto per quanto riguarda il ruolo degli ormai onnipresenti social network. Anche in questo caso un esempio può essere utile. Da alcuni mesi molti siti permettono usufruire dei loro contenuti dopo essersi autenticati tramite il profilo Facebook, Twitter, Google in sostituzione della creazione di un nuovo account: indubbiamente un'agevolazione per l'utente che sfrutta i propri dati esistenti in un social network senza dover aprire a una nuova procedura di identificazione, creare un nuovo ID e una nuova password. Tuttavia, non è da escludere che impiegando tecniche di *phishing* ormai collaudate un criminale possa attrarre svariati individui su un sito trappola al fine di carpire dettagli personali proprio dal profilo di Facebook, Twitter, ecc. impiegato per l'autenticazione e da lì innescare il meccanismo per sottrarre l'identità reale della vittima.

Inoltre, incertezze rimangono riguardo gli autori e le modalità di furto d'identità. Infatti, come visto sopra, in molti casi le vittime non sanno chi e come abbia sottratto loro l'identità. Se si esamina, dunque, tale fattispecie alla luce delle teorie razionali sulla criminalità (Becker, 1968; Brantingham & Brantingham, 1991; Cornish & Clarke, 1986) ci si rende conto come i reati d'identità divengano attraenti per gli autori perché vi sono pochi rischi di essere scoperti, sanzioni contenute, guadagno alto.

Per cercare di dare risposte più chiare a questi interrogativi e migliorare sia la conoscenza di questa realtà criminale, sia gli interventi preventivi e repressivi, può essere utile un approccio che parta dalle indagini di vittimizzazione già impiegate nel settore al fine di individuare gli elementi della commissione di un reato d'identità che possono identificare

due aspetti cruciali. In primo luogo esaminare i comportamenti degli utenti al fine di ridurre le opportunità che essi stessi inavvertitamente forniscono ai ladri d'identità. In altri termini capire ciò che, secondo la teoria delle attività di routine, rende la vittima un bersaglio adeguato e appetibile per il crimine (Cohen & Felson, 1979) al fine di predisporre contromisure efficaci (es. sistemi di *alert* per gli utenti).

In secondo luogo, ampliare la conoscenza delle modalità con cui sono perpetrati i reati d'identità, dividendo ogni furto/frode d'identità in fasi secondo lo schema dei c.d. *crime scripts* (Cornish D. B., 1994; Smith & Cornish, 2003). Tale approccio scompone un crimine in molte fase (ideazione, preparazione, commissione, fuga, ecc.) al fine di comprendere se vi siano degli schemi ricorrenti (*pattern*) che possono essere individuati al fine di predisporre interventi preventivi e/o repressivi. Una tecnica di questo tipo permetterebbe di determinare quali siano i meccanismi ricorrenti nei reati d'identità (ad es. uso massiccio del *phishing* o di spam) per elaborare strategie di intervento tese da un lato a rafforzare le difese delle possibili vittime e dall'altro ad aumentare i rischi per i criminali.

Bibliografia

Acoca, B. (2008). Online identity theft: a growing threat to consumer confidence in the digital economy. In D. Chryssikos, N. Passas, & C. D. Ram (Eds.), *The evolving challenge of identity-related crime: addressing fraud and the criminal misuse and falsification of identity* (pp. 74-75). Milano: ISPAC.

Acquisti, A., & Gross, R. (2009). Predicting Social Security numbers from public data. *Proceedings of the National Academy of Sciences (PNAS) , 106* (27), 10975-10980.

ADICONSUM. (2009). *Report 2009: Il furto d'identità nell'esperienza dei consumatori.* Osservatorio permanente sul furto d'identità. Roma: ADICONSUM.

ADICONSUM. (2010). *Report 2010: Il furto d'identità nell''esperienza dei consumatori*. Osservatorio permenente sul furto d'identità. Roma: ADICONSUM.

Becker, G. (1968). Crime and punishment: An economic approach. *The Journal of Political Economy, 76*, 169-217.

Brantingham, P. J., & Brantingham, P. L. (Eds). (1991). *Environmental Criminology.* Prospect Heights: Waveland Press.

Brown, G., Howe, T., Ihbe, M., Prakash, A., & Borders, K. (2008). Social networks and context-aware spam. *Proceedings of the 2008 ACM conference on computer supported cooperative work* (p. 403-412). New York: ACM.

CIFAS. (2010). *Digital Thieves - A special report on online fraud.* Londra: CIFAS.

Cohen, L., & Felson, M. (1979). Social change and crime rate trends: a routine activity approach. *American Sociological Review, 44* (4), 588-608.

Cornish, D. B. (1994). *The procedural analysis of offending and its relevance for situational prevention.* Monsey: Criminal Justice Press.

Cornish, D., & Clarke, R. (Eds). (1986). *The reasoning criminal.* New York: Springer.

Elliott, C. (2010, Giugno 13). In 'phishing' scams, purported acquaintances claim to be stranded abroad. *The Washington Post*.

Europol (2006). *OCTA - EU organised Crime Threat Assessment 2006*. Tratto il giorno 7 20, 2011 da www.europol.europa.eu/sites/default/files/publications/octa2006.pdf

FPEG. (2007). *Report on identity theft/fraud.* Fraud Prevention Expert Group. Bruxelles: Commissione europea.

FTC. (2011). *Data Book for January - December 2010*. Tratto il giorno 7 19, 2011 da http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2010.pdf

Gross, R., & Acquisti, A. (2009). Information revelation and privacy in online social networks. In D. Matheson (Ed.), *Contours of privacy* (pp. 197-218). Newcastle upon Tyne: Cambridge Scholars Publishing.

ITRC. (2009). *Identity Theft: The Aftermath 2008*. Tratto il giorno 07 17, 2011 da www.idtheftcenter.org/artman2/uploads/1/Aftermath_2008_20090520.pdf

Krishnamurthy, B., & Wills, C. E. (2010). On the leakage of personally identifiable information via online networks. *SIGCOMM Computer Communication Review, 40* (Gennaio), 112-117.

Labitzke, S., Taranu, I., & Hartenstein, H. (2011). What your friends tell others about you: low cost linkability of social network profiles. *The 5th SNA-KDD workshop '11*. San Diego.

Lampe, C., Ellison, N., & Steinfeld, C. (2007). A familiar face(book): profile elements as signals in an online social network. *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 435-444). New York: ACM.

McNally, M. M., & Newman, G. R. (2008). Editors' introduction. In M. M. McNally, & G. R. Newman (Eds.), *Perspectives on identity theft* (pp. 1-8). Cullompton: Willan Publishing.

McNally, M. M., & Newman, G. R. (Eds.). (2008). *Perspectives on identity theft.* Cullompton: Willan Publishing.

Patchin, J., & Hinduja, S. (2006). Bullies move beyond the schoolyard: a preliminary look at cyberbullying. *Youth Violence and Juvenile Justice, 4* (2), 148-169.

Smith, M. J., & Cornish, D. B. (2003). *Theory for practice in situational crime prevention.* Monsey: Criminal Justice Press.

Smith, P. K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., & Tippett, N. (2008). Cyberbullying: its nature and impact in secondary school pupils. *Journal of Child Psychology and Psychiatry, 49* (4), 376-385.

Synovate. (2007). *2006 Identity Theft Survey Report*. Tratto il giorno 7 18, 2011 da www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf

UN IEG. (2007). *Results of the second meeting of the Intergovernmental Expert Group to Prepare a Study on Fraud and the Criminal Misuse and Falsification of Identity.* Tratto il giorno 7 20, 2011 da www.unrol.org/files/E_CN_15_ 2007_8%5B1%5D.pdf

Wall, D. S. (2007). *Cybercrime: the transformation of crime in the digital age.* Cambridge: Polity Press.

Zaller, A. (2011, Gennaio 4). New law makes it illegal to impersonate others on social networking sites. *California Employment Law Report*.

Zetter, K. (2011, Aprile). Carder pleads guilty to fraud involving $36 million in losses. *Wired USA*.