RASSEGNA ITALIANA DI CRIMINOLOGIA
ANNO XIII N.1 2019

Frodi informatiche in Italia: un'esplorazione tramite l'*Hypothesis Testing Crime Analysis Approach*

Cyber fraud in Italy: an exploration through the "Hypothesis Testing Crime Analysis Approach"

Giacomo Salvanelli

Abstract
Cyber fraud seems to be a growing phenomenon, linked to the constant and impressive progress of technology. As such, this research wanted to explore through QGIS the regional distribution of cyber frauds by detecting any growing and/or decreasing trends underneath it. In regard to prevention, the methodology called 'Hypothesis Testing Crime Analysis Approach' was applied to identify the characteristics and data needed to develop hypotheses about both the underlying social causes of cyber fraud and the factors that make some individuals more vulnerable than others. The results revealed three factors overlapping with the growing cyber fraud rates in Italy: the age index, the lack of education in cyber prevention, the increasing number of internet users.

Key words: cyber crime • cyber fraud • QGIS • internet • Hypothesis Testing Crime Analysis Approach

Riassunto
Le frodi informatiche risultano essere un fenomeno crescente, legato al costante ed imponente progredire della tecnologia. Sul piano della prevalenza, questa ricerca ha cercato di esplorare, tramite il programma di mappatura QGIS, la distribuzione delle frodi informatiche regionali rivelando trends di crescita e/o decrescita. Sul piano preventivo, è stata applicata la metodologia analitica denominata 'Hypothesis Testing Crime Analysis Approach' per identificare caratteristiche e dati necessari a sviluppare ipotesi nei confronti sia delle cause sociali alla base delle 'cyber frodi' sia dei fattori che rendano alcuni individui vulnerabili. I risultati hanno rilevato tre fattori che coincidono con il tasso crescente delle 'cyber frodi' in Italia: l'indice di vecchiaia degli internauti, la mancanza di educazione in materia di cyber prevenzione, l'incrementato numero di internauti.

Parole chiave: cyber crime • frodi informatiche • QGIS • internet • Hypothesis Testing Crime Analysis Approach

Per corrispondenza: Giacomo SALVANELLI • *giacomo.salvanelli@alice.it*

Giacomo SALVANELLI • Founding Partner and Coordinator of the Criminology Department of MISAP Institute, PhD Candidate at TRANSCRIME, Università Cattolica del Sacro Cuore di Milan

DOI: 10.7347/RIC-012019-p18

1. Introduzione e Revisione della Letteratura

Le frodi informatiche fanno parte di un'ampia gamma di reati criminali denominata a livello internazionale 'cyber crime', la quale è divenuta senza dubbio una delle terminologie più frequentemente utilizzate nella criminologia del ventunesimo secolo. A tal proposito, per comprendere a fondo il vero significato di 'cyber crime', è necessario intendere la sottile linea di demarcazione che separa il concetto di 'cyber' da quello di 'crime' (Hassan et al, 2012). Il termine 'cyber' non è altro che un prefisso utilizzato per categorizzare un gruppo di idee, funzioni ed azioni che coinvolgono la realtà computazionale mentre l'espressione 'crime' rappresenta un'attività (singola o multipla) che contravviene le presenti ed accettate procedure normative della nostra società (Hassan et al, 2012). A tal proposito, i reati ascrivibili al gruppo del 'cyber crime' possono essere descritti come "tutti i crimini commessi in via telematica utilizzando un sistema computazionale come strumento chiave per colpire una o più vittime designate" (direttamente o indirettamente) (Joseph, 2006; Hassan et al, 2012; Florêncio & Herley, 2013).

Pertanto, se da un lato Internet ha fornito una serie di piattaforme utilizzabili in materia di aggiornamento e ricerca, dall'altro ha generato uno spazio virtuale entro cui i 'cyber criminali' si muovono liberi, arrivando a causare anche miliardi di dollari di danni. Ad esempio, come riportato da Hassan e colleghi (2012), la piattaforma *crime-research.org* ha messo in luce che già all'inizio del 2003 gli Stati Uniti avevano subito qualcosa come il 35,4% di tutti gli attacchi informatici registrati sul pianeta, seguiti dalla Korea del Sud con il 12,8%. Da un punto di vista preventivo, tuttavia, i paesi caratterizzati da alti livelli di 'cyber crime', come la Russia, sembrano aver reagito in modo piuttosto lento a questa nuova forma di illecito. Il risultato, come riportato successivamente anche da Guillane & Fortinet (2009) e da Anderson et al. (2012), è che molti cyber criminali hanno potuto (e possono ancora) prosperare in quei paesi mancanti di leggi sul 'cyber crime' dal momento che, a causa dell'assenza di una precisa demarcazione geografica (e legislativa) della realtà informatica, non vi sono né regole né autorità centrali che si assumano la responsabilità di garantire il rispetto delle normative online.

Inoltre, la natura multi-sfaccettata dei crimini informatici rende la loro identificazione spesso laboriosa. Ad esempio, il '*cyber terrorismo*' coinvolge qualsiasi atto rivolto allo sviluppo di paura attraverso il furto e la promulgazione di informazioni governative dal cosiddetto 'cyberspace' (Gross et al, 2016). Possiamo ricordare quanto accadde con l'intervento di 'Anonymous' (anonimo gruppo di hackers e attivisti informatici appartenenti alla sottocultura di internet) durante l'hackeraggio del dipartimento di polizia di Ferguson (Stati Uniti d'America). Essi fecero collassare l'intero sistema informatico della polizia per rilasciare impunemente il nome ed indirizzo abitativo del poliziotto che uccise Michael Brown, un 18enne afro-americano disarmato (Rogers, 2014; Perlroth, 2014), con lo scopo di scatenare un vero e proprio linciaggio. Diversamente, la '*cyber frode*' è un furto di dati personali ai danni di una persona o compagnia con lo scopo di ottenere un guadagno economico (Ionescu et al, 2011; Williams, 2007; Njanike, Dube & Mashanyanye, 2009; Rajasthan, 2013). Ad esempio, sono frequenti le tecniche di '*phishing*' (truffa informatica effettuata inviando un'e-mail al cliente per carpire dati riservati come il numero di carta di credito e password di accesso al servizio di home banking), mentre nel caso delle imprese tali frodi avvengono principalmente attraverso '*malware*' (codice malevolo che può essere diffuso attraverso programmi, documenti o messaggi di posta elettronica, in grado di rendere disponibili informazioni riservate e codici d'accesso al truffatore), a conferma di una specializzazione dei meccanismi di frode a seconda del tipo di clientela (Holt & Lampke, 2010). Infine, abbiamo il cosiddetto '*password sniffing*', il quale può essere definito come l'utilizzo di software o hardware per intercettare e registrare il traffico che passa attraverso una rete di computer (Freiermuth, 2011). Più precisamente, le persone dell'industria lo hanno descritto come un *"wire tap"* ("un tappo a filo") che consente di intercettare il traffico di rete (Freiermuth, 2011). Celebre fu il caso di Albert Gonzalez che si appropriò di 15 milioni di dollari attraverso il 'password sniffing' dei dettagli bancari di oltre 40 milioni di carte di credito, colpendo più di 250 istituzioni finanziari nel mondo. A questo proposito la domanda che sorge spontanea è: come avviene il processo di vittimizzazione online? Per rispondere a questa domanda il lavoro di Burgard & Schemblach (2013) sembra essere molto utile. Infatti applicando il concetto di 'frame analysis' di Goffman (1974, p. 13), hanno dimostrato che la frode è un'interazione strategica dove il frodante utilizza una sequela di informazioni ritenute poco importanti dalla vittima a suo vantaggio, lasciando intendere quindi una diversità percettiva nei confronti dello stesso oggetto (informazioni utili) (Burgard & Schemblach, 2013). La processualità vittimizzante presenta tre fasi, le quali sono strutturalmente equivalenti a quello che gli antropologi chiamano 'riti di passaggio' (Burgard & Schemblach, 2013). Nel primo stadio, la futura vittima viene isolata dalla percezione di minaccia così da spingerla ad abbassare i livelli di precauzione (Burgard & Schemblach, 2013). Precauzione che, se assente, sembra essere alla base di una maggiore (e non sorprendente) esposizione della vittima alla frode (Baumeister, 2002). Successivamente, il criminale intesse una superficiale ma effi-

cace rete di contatti illusori con la vittima per incrementare il suo senso di 'sicurezza illusoria' (Burgard & Schemblach, 2013). Nella terza fase, la vittima prende coscienza del suo ruolo in quanto parte lesa all'interno della truffa subita (Burgard & Schemblach, 2013).

Ciò che si evince dalla letteratura preesistente è che non solo la 'cyber fraud' è un fenomeno crescente in tutto il mondo, in quanto inevitabile conseguenza del massivo processo di digitalizzazione della nostra società, ma che anche le processualità della vittimizzazione ed "aggancio criminale" (Burgard & Schemblach, 2013) insite in essa possono essere di difficile identificazione ai più. Privati cittadini, banche, società, compagnie ed istituzioni finanziarie sono solo alcune delle realtà entro cui si può verificare un insieme di condotte virtualmente criminali che possono portare al furto di informazioni, di dati sensibili e di denaro. In aggiunta, la struttura polivalente della cyber fraud è coadiuvato dall'inesistenza di normative internazionali per la tutela dei vari clienti colpiti. Infatti, ciascuna nazione sembra dedicarsi alla creazione di misure di sicurezza interne che, per quanto efficaci, potrebbero essere rese ancora più incisive qualora ci fosse una maggiore collaborazione e confronto fra di esse a livello internazionale. Inoltre la natura non fisica di questa categoria di reati non permette una vera e propria definizione sociologica del fenomeno da cui ne deriva che, qualunque metodo sembra risultare inadeguato in quanto svincolato da qualsivoglia concettualizzazione informatica. Proprio su quest'ultimo punto Jaishankar (2007; 2010) introduce l'interessante teoria della 'Space Transition' per spiegare come in realtà qualsiasi forma di illecito cibernetico può essere importato nel mondo fisico e viceversa, ed è proprio da qui che si deve partire. In altre parole, come sottolineato da Holtfreter et al. (2008) e da Pratt et al. (2010) si deve cominciare dalle opportunità criminali offerte dal mondo digitale e come queste si vadano ad integrare coi fattori sociali-ambientali circostanti.

Pertanto questo articolo vuole esplorare il fenomeno della 'cyber frode' in Italia attraverso una prospettiva integrata di natura scientifica-sociale analizzando i dati forniti dal Ministero dell'Interno oltre a quelli provenienti da altre fonti online per il periodo intercorso fra il 2014 e il 2016. In aggiunta, per garantire una rappresentazione geodetica del fenomeno, questa analisi verrà supportata dall'applicazione del programma di mappatura geografica di nome QGIS (Quantum Geographical Information System) che garantirà la realizzazione di alcune 'choropleth maps' relative l'incidenza regionale delle frodi informatiche. In altre parole, sarà possibile mettere in evidenza, tramite dei marcatori geografici, la distribuzione delle frodi informatiche regionali rivelando così non solo quali regioni sono state le più colpite ma anche eventuali trends di crescita/decrescita. Successivamente questo lavoro adopererà una metodologia analitica per esplorare le cause e trends criminologici sottostanti la distribuzione regionale di tali reati informatici. Questa metodologia chiamata 'Hypothesis Testing Crime Analysis Approach', largamente utilizzata nel Regno Unito dal centro di scienza del crimine chiamato 'Jill Dando Institute of Security and Crime Science', sarà presentata in dettaglio nella prossima sezione. Questa tecnica verrà applicata ai risultati geo-analitici prodotti a seguito della fase operativa (mappatura tramite QGIS) con lo specifico obiettivo di vedere se essa può fornire una chiave di lettura del fenomeno per incrementare le possibilità di identificarne caratteristiche e trends necessari a sviluppare potenziali ipotesi nei confronti sia delle cause sociali alla base delle 'cyber frodi' sia di eventuali fattori che rendano alcuni individui (o aziende) 'virtualmente' vulnerabili. Una maggiore comprensione socio-criminologica infatti permetterebbe di definire come questa tipologia di reato sia tanto endemica, aprendo così le porte ad eventuali progetti di utilità sociale per intervenire sul fenomeno con una maggiore consapevolezza scientifica, passando da un'azione contenitiva ad una preventiva.

1.1 *Hypothesis Testing Crime Analysis Approach*

Man mano che il paradigma centrale delle tecniche d'indagine delle forze di polizia britanniche si è evoluto, una nuova metodologia analitica del funzionamento criminale è stata sviluppata dal centro di scienza del crimine della University College of London al fine di migliorare il contenuto esplicativo di eventuali prodotti analitici, come ad esempio la profilazione di un dato fenomeno criminale (Chainey, 2014). Più precisamente tale nuova metodologia si prefigge lo scopo di identificare un numero (3-5 max) di cause plausibili ('ipotesi') per spiegare l'origine ed il mantenimento del fenomeno criminale studiato ed utilizzarle per indirizzare in modo adeguato l'analisi dello stesso (Chainey, 2014). Testare le 'ipotesi' permette all'analista del crimine di focalizzare la propria analisi su un piano prettamente pragmatico rivolto alla comprensione del 'why?' (perché?) di quel dato fenomeno, dal quale successivamente si potrà estrapolare il 'who?' (chi viene coinvolto?), il 'what?' (cosa succede effettivamente?), il 'where?' (dove accade il fenomeno?), il 'when?' (quando accade?) ed infine il 'how?' (come si manifesta?) (Chainey, 2014).

Pertanto, è importante sottolineare come tale approccio possa aiutare a comprendere (ed evidenziare) in modo più efficace la natura di un fenomeno criminale (Chainey, 2014). A tal proposito, questo metodo si basa su 4 fasi ben distinte (Chainey, 2014):

– *The Overview* (La panoramica del fenomeno in questione)
  Questa fase implica una chiara definizione del fenomeno criminale da analizzare. Infatti, dovrebbe determinare la grandezza, la portata, le tendenze e tutte le informazioni specifiche che aiutano più chiaramente a identificare il problema. La panoramica deve essere concisa (ossia un massimo di tre pagine in lunghezza), ma dovrebbe fornire comunque dettagli sufficienti per la fase 2 (Chainey, 2014).
– *Deciding on Hypotheses* (La scelta delle eventuali ipotesi analitiche)
  Questa fase presuppone la formulazione di ipotesi che spieghino le potenziali cause alla base del problema ana-

lizzato. Esse devono essere chiare, concise e temporalmente orientate al periodo durante il quale il fenomeno criminale è emerso. Il numero ideale è quello di 3-5 ipotesi massimo (Chainey, 2014).

– *Analysis* (L'analisi effettiva e validazione delle ipotesi)
  L'obiettivo primario di questa fase è fornire una qualche evidenza che possa andare a confermare (o mettere in discussione) le ipotesi formulate nella fase precedente. Il tipo di analisi condotta deve dipendere dalla natura stessa delle ipotesi. Ad esempio, se un'ipotesi afferma che un recente aumento di furti residenziali è legato ad un aumento delle case rimaste insicure (perché i residenti lasciano le finestre aperte a causa di un recente aumento delle temperature), l'analisi dovrà identificare se c'è stato o meno un recente aumento delle temperature proprio durante le notti in cui vi è stato l'aumento dei furti. Questo metodo permetterà così di individuare dove possono esserci eventuali lacune analitiche, orientando in modo più preciso future indagini (Chainey, 2014).
– *Conclusions and response recommendations* (Conclusioni e raccomandazioni per interventi futuri)
  Questa fase porta alla costruzione di prove che possono contribuire a spiegare le cause del fenomeno criminale e, a sua volta, rendere più facile l'interpretazione di tali risultati durante le fasi conclusive. Infatti, i risultati delle analisi vengono messi a confronto coi dati iniziali avviando così un processo valutativo retroattivo che cercherà di validare le supposizioni iniziali così da concludere l'esplorazione, definizione e comprensione del fenomeno criminologico (Chainey, 2014).

L'analista del crimine è responsabile delle fasi 1 e 3, mentre le fasi 2 e 4 spettano ai cosiddetti 'policy makers', i quali sono coloro che hanno un interesse concreto nei confronti del problema e/o sono in una posizione di responsabilità per poter fare qualcosa a riguardo (Chainey, 2014).

Dal momento che, per la natura stessa di questa ricerca, ricopriremo sia il ruolo di analisti del crimine sia quello di potenziali 'policy makers', procederemo al completamento di tutte le quattro fasi in modo da realizzare un'esaustiva 'Hypothesis Testing Analysis' sul fenomeno delle 'cyber frodi' in Italia. Tuttavia, considerando che qualunque risultato, inferenza o teorizzazione sarà basato su materiali, dati e informazioni preesistenti (secondary data), è importante sottolineare come la 4' fase poggerà su raccomandazioni di natura teorico-preventiva piuttosto che sulla costruzione di prove empiriche consolidate. Infatti, il presente studio vuole costituire il primo passo verso un futuro processo esplorativo che possa, attraverso l'utilizzo di dati primari di ricerca, fornire metodi e conoscenze utilizzabili con lo scopo di prevenire il sopraggiungere di eventuali frodi informatiche.

Come precedentemente illustrato, l'analisi delle 'cyber frodi' in Italia partirà con una loro panoramica (*overview*) con lo specifico obiettivo di identificarne la grandezza, portata, trends e tutte le informazioni specifiche che possano aiutare a capire più chiaramente la loro natura.

1.2 *Overview: 'Cyber frodi' in Italia*

In Italia i dati del 2016 emersi dalle statistiche provinciali e regionali sulle attività delittuose rivelano una significativa riduzione dei tassi di criminalità generale rispetto al 2014 (-14,20%) (Gianotti, 2016). Per esempio, le estorsioni sono calate del 17,95%, i furti con destrezza del 13,94%, i furti con strappo del 36,36%, i furti di autovetture del 16,59%, i furti in abitazione del 24,96%, i furti in esercizi commerciali del 24,86%, ed infine i reati di riciclaggio e impiego di denaro/beni/utilità di provenienza illecita addirittura del 75% (Gianotti, 2016).

Tuttavia, le frodi informatiche sembrano essere l'unica categoria delittuosa che invece di ridursi è cresciuta significativamente ed inoltre solo il 18% di chi commette 'cyber frodi' risulta essere conclusivamente smascherato (Custodero, 2007). Ad esempio, nel quadriennio 2011-2014 è stato rilevato che questa categoria 'relativamente' nuova di illeciti ha presentato tassi crescenti in Italia (+23%), sebbene in misura minore rispetto a quelli dell'Europa Occidentale (+30%), delle Americhe (Nord +41% e Sud +35%), dell'Africa (+50%) e dell'Europa dell'Est (+39%) (Cancellato, 2014). A tal proposito calando la presente panoramica in un'ottica regionale, nel 2015 è stato rilevato un aumento delle 'cyber frodi' in tutte le regioni italiane tranne la Calabria, la quale ha visto invece una riduzione del 1,91% rispetto al 2014 (Gianotti, 2016). Osservando la figura 1, rappresentante la media di frodi informatiche ogni 100mila abitanti, si nota l'esistenza di due aree con una maggiore incidenza territoriale: uno di essi localizzabile fra Molise e Campania con rispettivamente 309 e 297 reati ogni 100mila abitanti, ed un altro a cavallo fra Liguria, Valle D'Aosta, Piemonte, Friuli-Venezia Giulia ed Emilia Romagna con rispettivamente 323, 291, 274, 272 e 262 reati ogni 100mila abitanti (Gianotti, 2016).

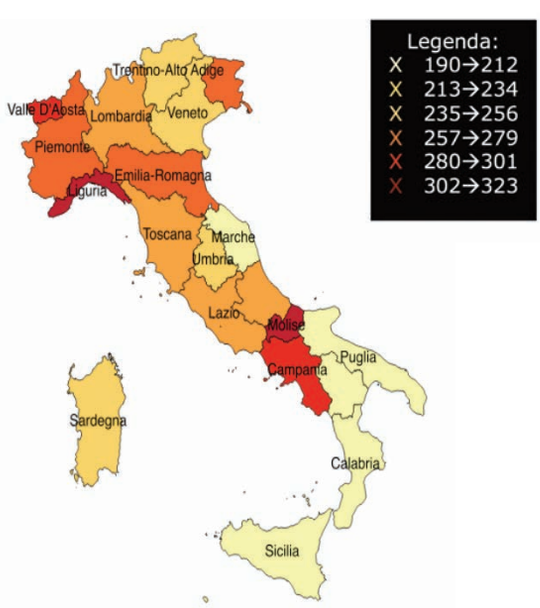

Fig.1 Media delle Frodi Informatiche denunciate (2014-2016) nelle regioni italiane ogni 100mila abitanti

I dati emersi da questa analisi nazionale sembrano collidere con quanto riportato dall'Associazione Bancaria Italiana (ABI) nel 2016, la quale riferisce che "l'attività di difesa delle banche italiane contro le frodi informatiche è sempre più efficace: nel 2015, oltre il 94% del volume economico associato ai tentativi di frode è stato bloccato con successo. Un caso di frode stimato ogni 166mila operazioni eseguite via Internet dalla clientela Retail" (ABI, 2016). Tuttavia proprio nel marzo del 2017, Vincenzo Francese, amministratore unico di AXERTA (il primo network investigativo in Italia), ha contrariamente affermato come i crimini informatici e l'infedeltà di dipendenti, dirigenti e amministratori siano invece al primo posto (67%) tra le frodi più temute dalle imprese italiane (Destri, 2017). A conferma di quest'ultimo, nel mese di agosto 2017, un'importante indagine del Nucleo di Polizia Tributaria della Guardia di Finanza di Brescia, coordinata dalla Procura della Repubblica, ha rintracciato 21 siti internet che diffondevano dati illecitamente, sotto pagamento di Bitcoin (valuta digitale non rintracciabile) (Buizza, 2017). Più nel dettaglio, secondo quanto riportato da Buizza (2017), questa operazione ha "svelato una forma di frode sempre più diffusa in rete. Infatti, i siti internet rendevano disponibili centinaia di migliaia di numeri di carte di credito, credenziali per l'accesso ai servizi di home banking di clienti di vari istituti

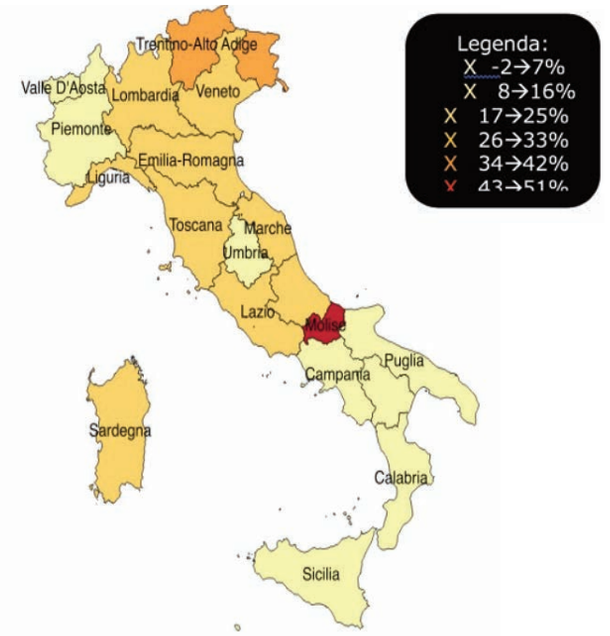

Fig. 2. Percentuale di crescita media delle frodi denunciate (2014-2016) nelle regioni italiane ogni 100mila abitanti.

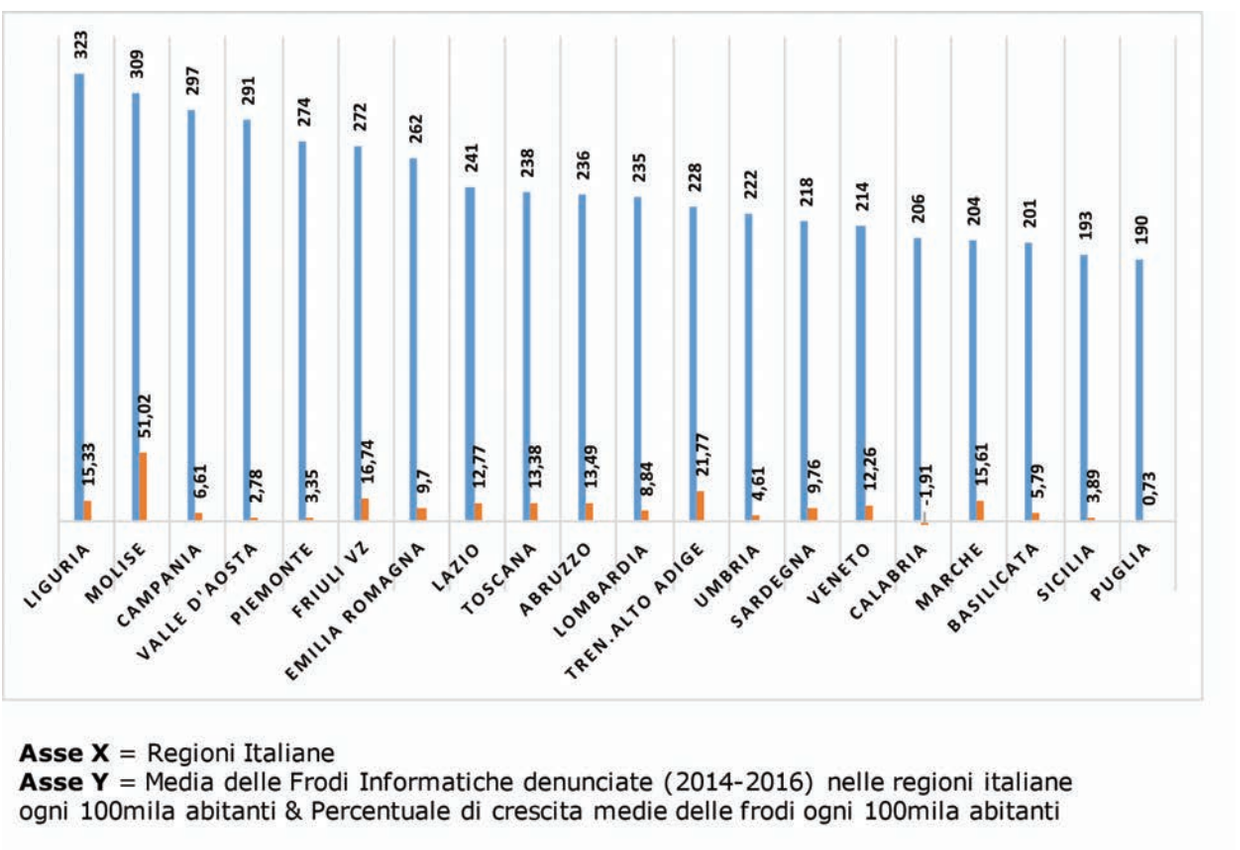

Grafico 1

bancari, nonché le modalità da seguire per ottenere illecitamente rimesse di denaro mediante circuiti di money transfer". Inoltre, come riportato da Giordano (2015) e dalla MarkMonitor (azienda leader nella protezione del brand online) (EL, 2016), vi sono innumerevoli nuove forme di cyber frode, le quali vengono quasi completamente ignorate da privati e aziende nonostante la loro significativa efficacia. Ad esempio le tecniche 'Man-In-The Middle', false richieste di reimpostare la password, falsi profili sui social networks e molte altre ancora sono alla base di un significativo studio effettuato dalla MarkMonitor (EL, 2016), il quale ha rilevato che circa il 45% dei consumatori in Italia, Stati Uniti, Regno Unito, Germania, Francia, Danimarca, Spagna, Svezia e Paesi Bassi è stato cyber frodato almeno una volta negli ultimi quattro anni.

Alla luce di quanto detto fino ad ora, potremmo affermare che, a prescindere dal 'target' di vittime fra privati e aziende, le controversie concettuali emerse nel definire l'entità di questo fenomeno lasciano trasparire una sostanziale difficoltà nel capire sia le cause sia le manifestazioni delle 'cyber frodi'. Mentre da un lato, come evidenziato dall'ABI, è possibile notare un'importante investimento di denaro ed energie per quanto concerne un contenimento 'situazionale' delle frodi, dall'altro questo intervento sembra mancare di una effettiva comprensione della natura socio-criminologica delle stesse, il quale invece permetterebbe lo sviluppo di un'ottica preventiva più a lungo raggio.

1.3 *Deciding on Hypotheses: Ipotesi socio-criminologiche*

A seguito della panoramica fornita nella sezione precedente, procederemo ora alla formulazione di alcune ipotesi che cercheranno di spiegare le potenziali cause scatenanti le 'cyber frodi' in Italia, prestando attenzione anche a caratteristiche regionali. Queste ipotesi cercheranno di essere chiare, concise e geograficamente orientate ai luoghi nei quali le 'cyber frodi' sono emerse con maggiore intensità.

***Prima Ipotesi* (regionale)**
L'indice di vecchiaia (grado di invecchiamento di una popolazione) è proporzionale al numero di frodi. In altre parole, una maggiore frequenza di 'cyber frodi' può essere trovata nelle regioni con l'indice di vecchiaia più alto.

***Seconda Ipotesi* (nazionale)**
Il crescente uso di tecnologie si accompagna ad una bassa attenzione da parte degli internauti verso la cyber prevenzione e ciò si verifica in concomitanza di un fenomeno crescente come quello delle frodi informatiche.

***Terza Ipotesi* (nazionale)**
L'avvento degli Smartphone e Tablet ha portato ad un numero maggiore di individui che settimanalmente navigano e/o fanno acquisti in rete (non più solo dal terminale). L'aumento della frequenza di acquisti online è proporzionale alla crescita di frodi denunciate nell'ultimo triennio.

2. Analisi dai Dati per la verifica delle ipotesi (*Testing Hypotheses*)

In questa sezione si cercherà di fornire una qualche evidenza empirica poggiante su dati secondari prodotti da precedenti studi e/o ricerche nel tentativo di confermare o mettere in discussione le tre ipotesi formulate. In altre parole, la verifica di ciascuna delle seguenti ipotesi non presuppone né la costruzione né l'affermazione di un nesso causale fra le variabili coinvolte, ma semplicemente cercherà di evidenziare se esiste una potenziale comparazione positiva fra di esse.

***Prima Ipotesi* (regionale)**
La verifica della prima ipotesi presuppone di capire se l'indice di vecchiaia regionale (grado di invecchiamento di una popolazione) è proporzionale al numero di frodi registrate. Più precisamente l'indice di vecchiaia è rappresentabile dalla formula ($P^{3}65$ / $P\mathcal{L}14$)*100 dove P indica la popolazione del territorio in oggetto; $^{3}65$ e $\mathcal{L}14$ le fasce di età della detta popolazione da utilizzare per il calcolo dell'indice. A tal proposito, una ricerca commissionata da Centrale Rischi d'Intermediazione Finanziaria (Crif) a *Smart Research* ha rilevato che su un campione di persone di età compresa fra i 45 e 54 anni più del 50% sono caduti nella trappola del phishing (Centrale Rischi d'Intermediazione Finanziaria, 2015). Quest'ultimo dato non sorprende considerando il numero crescente di italiani over 50 che dal 2014 si connette online con regolarità. Più precisamente sono gli over 50 a far segnare i maggiori progressi: il 26,6% degli italiani tra i 50 ed i 74 anni d'età si sono connessi alla rete almeno una volta, con un incremento del 46,5% rispetto al 2015 degli utenti che si connettono tramite Smartphone (Cultur-E, 2017; Audiweb, 2016). In altre parole, seppure con un leggero ritardo rispetto ad altri paesi d'Europa, anche gli italiani over 50 hanno iniziato a valorizzare il mondo online e tutte le sue potenzialità (Cultur-E, 2017; Audiweb, 2016). Tuttavia, la positività di questo evento potrebbe essere inficiata dal fatto che l'acuita presenza di 'anziani' online causerebbe un aumento della probabilità di frodi subite dagli stessi data la loro potenziale scarsa competenza ed esperienza in materia di web-surfing.

Infatti, osservando la figura 3 è possibile notare come sembra esserci effettivamente un'effettiva proporzione fra l'indice di vecchiaia regionale (indicante lo stato di invecchiamento della popolazione) e la frequenza di cyber frodi registrate. Ad esempio, stando ai dati rilasciati da UrbiStat (2017) per il triennio 2014-2016, si nota come le regioni maggiormente colpite da reati informatici siano proprio quelle con un indice di vecchiaia più alto. Più nel dettaglio, è interessante osservare come la Liguria (Indice di Vecchiaia (I.V.): 249,8), il Friuli-Venezia Giulia (I.V.: 208,8), il Molise (I.V.: 206,9), la Toscana (I.V.: 198,60) ed il Piemonte (I.V.: 197,60) non siano solo le cinque regioni con il più alto stato d'invecchiamento della popolazione ma siano anche cinque fra le regioni più colpite dalle frodi informatiche, ricoprendo rispettivamente la prima posizione (Liguria), la seconda (Molise), la quinta (Piemonte), la sesta (Friuli-Venezia Giulia) e la nona (Toscana) per numero di reati denunciati alle forze giudiziarie (vedi grafico 2).

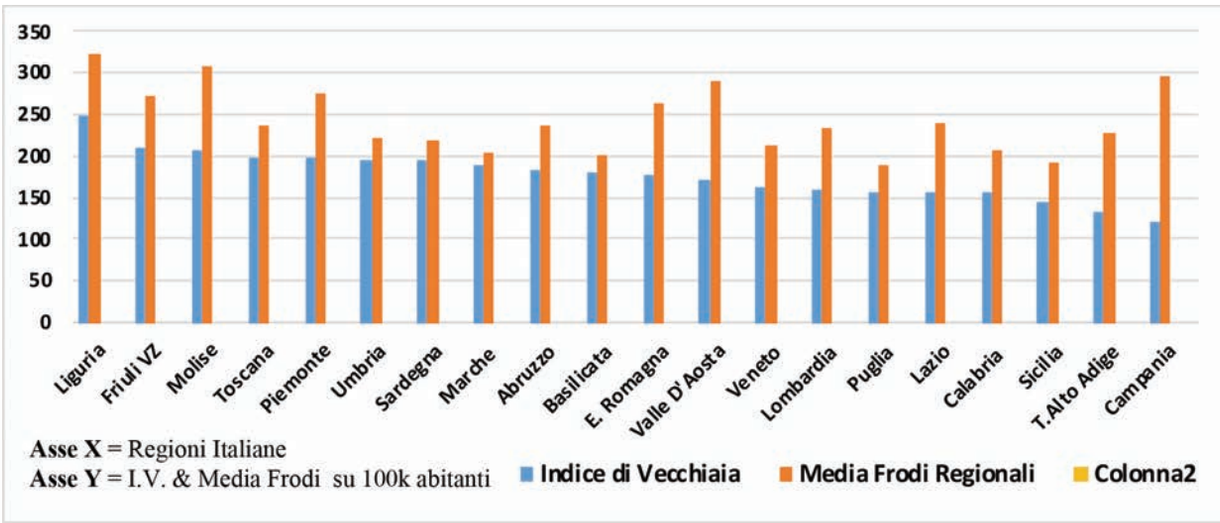

Grafico 2: Comparazione Grafica fra Indice di vecchiaia (I.V.) e la media delle frodi denunciate (2014-2016) nelle regioni italiane ogni 100mila abitanti.

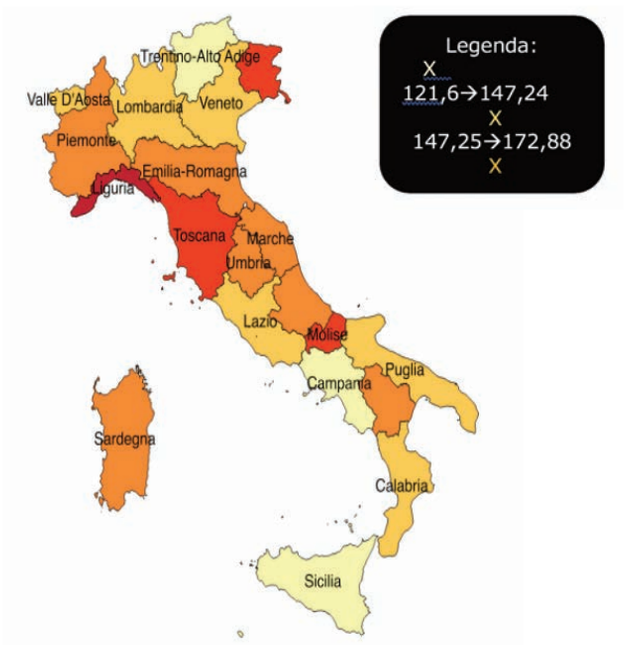

Fig. 3. Indice di Vecchiaia a livello Regionale (2014-2016)

Inoltre, come già evidenziato sia dalla fig. 2 e sia dal grafico 1 (p. 8) - rappresentanti la percentuale di crescita regionale del numero di cyber frodi denunciate nel triennio 2014-2016 - vi è un aumento davvero significativo in gran parte delle regioni del centro-nord Italia con una percentuale compresa fra l'8,85% ed il 21,78%, con il Molise che sorprendentemente presenta un tasso di crescita rasentante il 52% in soli due anni.

Pertanto questi dati sembrano rimandarsi a quelli messi in luce dalla figura 3; l'esistenza di una significativa proporzione fra indice di vecchiaia e percentuale di crescita di cyber frodi infatti sembrerebbe nuovamente confermata.

***Seconda Ipotesi* (nazionale)**

La verifica della seconda ipotesi presuppone di capire se nonostante l'ampio uso di tecnologie, vi è ancora una ridotta attenzione da parte degli internauti verso la cyber prevenzione e che ciò si verifica anche in concomitanza di un fenomeno crescente come quello delle frodi informatiche. A tal riguardo, una ricerca realizzata dalla Centrale Rischi d'Intermediazione Finanziaria nel 2015 ha rilevato come nel triennio 2014-2016 vi siano state circa 26mila frodi creditizie ai danni dei consumatori, con danni fino a 162 milioni di euro (Corriere Comunicazioni, 2015). Tuttavia nonostante sia stata rilevata una maggiore consapevolezza della gravità delle situazioni che possono essere generate dalle suddette frodi, circa due terzi degli intervistati sembra essere comunque poco o per niente attento alla diffusione dei propri dati sul web (Corriere Comunicazioni, 2015; PLUS 24 Ore, 2015). Infatti, è interessante notare come nonostante il 68,4% degli intervistati conosca il fenomeno e i rischi che questo tipo di frode informatica comporta, solo il 42% apparrebbe davvero attento alla diffusione dei propri dati sul web (Corriere Comunicazioni, 2015; PLUS 24 Ore, 2015). A tal proposito è stato messo in luce che non solo il 58% di intervistati immette in modo indiscriminato dati personali in rete ma il 28% di esso lo fa senza nemmeno tutelarli a seguito del upload (Corriere Comunicazioni, 2015; PLUS 24 Ore, 2015).

Più precisamente e contrariamente a quanto si potrebbe pensare, anche tra gli utenti con maggiore propensione agli acquisti online non c'è una particolare attenzione alla tutela dei dati personali; infatti il 34% di chi fa almeno due acquisti online dichiara di non essere per nulla attento alla diffusione delle proprie informazioni (Corriere Comunicazioni, 2015). Questo potrebbe essere spiegato dal fatto che la tutela degli strumenti con cui si accede alla rete e la consapevolezza di proteggere i propri dati sulle piattaforme di navigazione risulta poco diffusa (Corriere Comunicazioni, 2015). Ad esempio solo il 37,6% ha dichiarato di aver investito risorse economiche per servizi che siano dedicati

alla protezione dati, mentre il 16,6% degli utenti non fa assolutamente nulla a riguardo, se non evitare di scaricare file o link sospetti (Corriere Comunicazioni, 2015).

In aggiunta, un dato piuttosto interessante emerso da tale ricerca è che i più giovani si dimostrano generalmente meno preoccupati dei possibili rischi (Corriere Comunicazioni, 2015). Infatti, nella fascia compresa tra i 18 e 24 anni solo il 7,5% degli utenti dichiara di investire in un servizio di protezione a pagamento sempre aggiornato, contro una quota del 49% nella fascia dai 45 ai 54 anni (Corriere Comunicazioni, 2015). Tuttavia, si può affermare che queste ultime percentuali potrebbero anche dipendere dalla maggiore competenza dei giovani appartenenti alla 'virtual generation' in materia di web-knowledge ('conoscenza del mondo online'), i quali sentendosi capaci e competenti in materia di navigazione vedrebbero come superflue eventuali spese extra in tema di protezione dati. Al contrario, gli 'anziani' potrebbero risultare maggiormente propensi all'acquisizione di programmi di protezione dati proprio a causa della loro minore conoscenza del web che li farebbe sentire maggiormente esposti ad eventuali frodi, essendo pertanto disposti ad investire denaro in misure di sicurezza; una sorta di 'scaff-holding' informatico esterno.

Similarmente a quanto illustrato fino ad ora, un altro studio che sembra confermare una sostanziale negligenza da parte dei consumatori online è la ricerca Total Retail 2016 condotta dalla PricewaterhouseCoopers su 23.000 web consumatori in 25 paesi (PricewaterhouseCoopers, 2017). In Italia, alla domanda 'come riduce i rischi legati al problema di sicurezza e frodi online?', le risposte dei consumatori hanno rilevato dati allarmanti che sembrano confermare la seconda ipotesi della presente ricerca. Infatti, il 42% ha confermato di scegliere frequentemente anche siti poco credibili e autorevoli pur di completare l'acquisto pattuito, il 41% sceglie spesso fornitori di servizi a pagamento che non conosce, il 57% ha rilevato di rivolgersi anche ad aziende sconosciute, il 60% non utilizza una carta di credito che offra protezione per gli acquisti, il 65% spesso clicca su finestre pop-up per curiosità, il 66% clicca su pubblicità, il 70% utilizza la medesima password per ciascun sito web su cui è registrato, il 73% fornisce più dati di quanti ne sarebbero necessari, il 77% conferma i dati di geo-localizzazione richiesti da alcuni siti web, il 79% non legge accuratamente le norme sulla privacy ed infine il 91% effettua acquisti anche da 'retailer' esteri (PricewaterhouseCoopers, 2017) (vedi grafico 3).

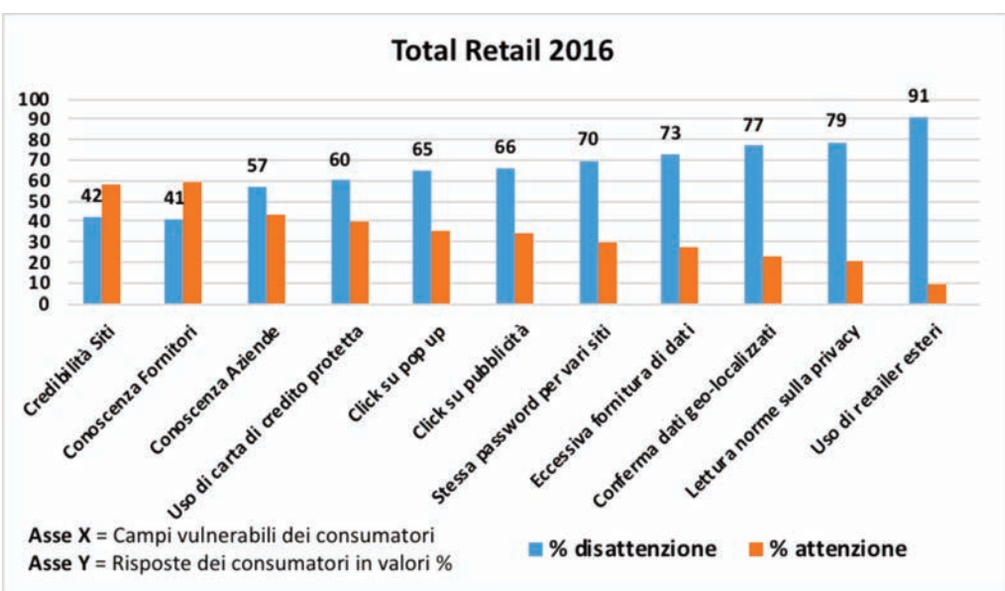

Grafico 3: Percentuale attenzione/disattenzione consumatori italiani online

Si può pertanto arrivare alla conclusione che, nonostante l'ampio uso di tecnologie, vi è ancora una ridotta attenzione da parte degli internauti verso la cyber prevenzione e che ciò si verifica anche in concomitanza di un fenomeno crescente come quello delle frodi informatiche. Tuttavia assolutizzare un nesso causale e temporale fra le frodi informatiche e la poca attenzione dei web-surfers non può essere ancora realizzato in modo definitivo.

***Terza Ipotesi* (nazionale)**

La verifica della terza ipotesi presuppone di capire se l'aumento della frequenza di acquisti online, coadiuvato anche dall'affermazione mondiale degli Smartphone, è proporzionale rispetto alla crescita di frodi denunciate nell'ultimo triennio. A tal proposito, Idealo Magazine nel 2016 ha evidenziato una crescita dell'e-commerce del 18% rispetto al 2015 (Idealo Magazine, 2017). Più precisamente nel 2016

la quota del commercio online in Italia (21 miliardi di euro) si aggira intorno al 3,6%, a fronte di un valore complessivo degli acquisti effettuati dagli italiani pari al 12% del mercato europeo (Idealo Magazine, 2017): un potenziale di crescita che negli ultimi anni ha acquisito una dimensione piuttosto notevole.

Alla luce di ciò, Idealo (piattaforma di shopping comparativo dedicata al risparmio digitale in Italia), ha avviato una collaborazione di ricerca con la Survey Sampling International (SSI) (uno dei principali fornitori mondiali di soluzioni per il campionamento e le ricerche di mercato online) con lo specifico scopo di indagare tale processo trasformativo (Idealo Magazine, 2017). L'indagine demografica ha coinvolto 1.000 acquirenti digitali italiani, i quali hanno costituito un campione piuttosto rappresentativo della popolazione sul web, ovvero il 63,2% degli italiani (Idealo Magazine, 2017). Infatti, il suddetto numero di partecipanti è stato ben stratificato in base alle variabili demografiche: età, genere, livello d'istruzione e regione (Idealo Magazine, 2017).

I dati emersi hanno rilevato che l'81% degli acquirenti digitali italiani effettua in media almeno un acquisto online al mese, un valore leggermente superiore a quello evidenziatosi nel contesto di un sondaggio analogo commissionato da Idealo nel Regno unito (76%). Secondo i dati provenienti da questa 'survey', è stato possibile stimare l'entità della trasformazione tecnologica e sociale del consumo online sulla base della frequenza degli acquisti elettronici effettuati: intensivi (una o più volte alla settimana: 28,6%), assidui (una o più volte al mese: 51,4%), abituali (una o più volte a trimestre: 33,5%) e sporadici (una o due volte all'anno: 4,2%) (Idealo Magazine, 2017). Questa segmentazione ha rilevato come alla guida del mercato digitale vi siano gli acquirenti 'assidui' (Idealo Magazine, 2017). Infatti, sembra che 1 su 2 e-consumatori acquista online almeno 3 volte al mese, un dato significativo che pertanto sembra spiegare l'incremento percentuale (18%) del numero di internauti rispetto al 2015 (Idealo Magazine, 2017).

Inoltre, a conferma di quanto emerso fino ad ora, uno studio dell'osservatorio Mobile B2c Strategy del Politecnico di Milano indica che nel 2016 i consumatori italiani dedicano sempre più tempo alla navigazione Internet via Mobile: 6 minuti su 10 passati online provengono dagli Smartphone con oltre 25 milioni di persone che mensilmente navigano dai propri Smartphone (pari circa al 70% degli utenti internet complessivi) (Osservatori.Net, 2017). Tale valore è cresciuto a doppia cifra rispetto al 2015, a differenza degli utenti desktop che sono invece in calo (Osservatori.Net, 2017). Inoltre è interessante notare come sia alta la percentuale dei 'Mobile Surfers' che non disattivano mai la connettività dei propri Smartphone: oltre due terzi (68%) ha il wi-fi sempre attivo, mentre la percentuale scende a poco più di un terzo (37%) per la geo-localizzazione e al 19% per il bluetooth (Osservatori.Net, 2017) (vedi grafico 4).

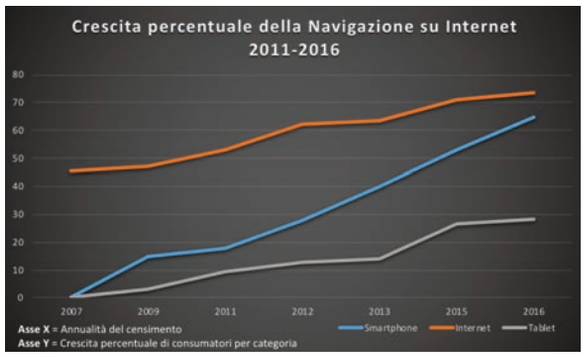

Grafico 4: crescita percentuale della navigazione su Internet 2011-2016 (Zunino, 2016).

Ancora, questi dati hanno trovato conferma nei risultati emersi da altre due ricerche. La prima presentata dal Corriere Comunicazioni nel 2016, ha riferito che sono 18,8 milioni gli E-shopper in Italia che hanno comprato sulla rete nei primi mesi del 2016 e che 12,8 milioni di essi hanno acquistano online almeno una volta al mese (Corriere Comunicazioni, 2016). In altre parole, nello spazio di 5 anni si è passati da 9 milioni di acquirenti online a quasi 19 milioni, raggiungendo un significativo 21% di acquisti realizzati solo tramite Smartphone evidenziando la repentina e forte ascesa della cosiddetta 'app-economy' (Corriere Comunicazioni, 2016). La seconda, condotta da Netcomm (consorzio del commercio elettronico italiano), citata de Enrico Netti (2017) in un articolo del Sole 24ore, ha messo in luce una crescita del 20% del e-commerce. Più precisamente sembra che questo sia il miglior incremento dal 2010, sfiorando di poco il raddoppio rispetto ai 12,6 miliardi del 2013 (Netti, 2017). Appare pertanto evidente la crescita esponenziale del numero di acquirenti online, i quali non solo sono cresciuti del 26% nel triennio 2014-2016 ma sono anche aumentati del 25% tra quelli classificabili come clienti abituali delle vetrine online (Netti, 2017), confermando quindi i dati riportati dalla Idealo Magazine e Survey Sampling International (SSI). Pertanto alla luce dei numeri emersi fino ad ora si può affermare innanzitutto che vi è stato un 'boom' delle tecnologie da navigazione e che, in secondo luogo, il parallelo (ed inevitabile) incremento della frequenza di acquisti online (+26% rispetto al 2014) risulta significativamente proporzionale rispetto alla crescita di frodi informatiche denunciate nell'ultimo triennio (+ 23% rispetto al 2014).

Conclusioni e Future Raccomandazioni

In quest'ultima fase si cercherà di fornire un'interpretazione conclusiva dei risultati ottenuti fino ad ora. Questi ultimi verranno messi a confronto con le supposizioni iniziali avviando così un processo valutativo-retroattivo che cercherà di completare l'esplorazione, definizione e comprensione del fenomeno criminologico delle 'cyber frodi' in Italia.

Come precedentemente illustrato, le 'cyber frodi' sem-

brano costituire l'unica categoria delittuosa italiana in crescita rispetto al 2014. Più precisamente, nell'ultimo anno e mezzo è stato rilevato un aumento delle 'cyber frodi' in tutte le regioni italiane tranne la Calabria, con due importanti punti di incidenza territoriale localizzabili fra Molise e Campania. Inoltre è stata rilevata una percentuale di crescita significativa delle stesse in gran parte delle regioni appartenenti al centro-nord Italia, tra le quali emerge una regione del sud: il sorprendente Molise con un +51,02% in soli tre anni (2014-2016). A seguito di questa panoramica, c'è stata la formulazione di tre ipotesi. Innanzitutto che l'indice di vecchiaia regionale (IV) fosse proporzionale al numero di frodi informatiche. Successivamente che, nonostante l'ampio uso di tecnologie, vi è ancora una ridotta attenzione da parte degli internauti verso la cyber prevenzione e che ciò si verifica in concomitanza di un fenomeno crescente come quello delle frodi informatiche. Infine, che l'aumento della frequenza di acquisti online fosse proporzionale rispetto alla crescita di cyber frodi denunciate nell'ultimo triennio (2014-2016).

L'analisi delle tre ipotesi ha portato ad una loro sostanziale conferma. Innanzitutto, è stato evidenziato che di pari passo con l'aumento delle frodi informatiche nell'ultimo triennio vi è stato non solo un significativo aumento di cybernauti di età compresa fra i 45 e 74 anni ma anche un loro importante tasso di vittimizzazione (50%), specialmente per quanto riguarda persone di età compresa fra i 45 e 54 anni (Centrale Rischi d'Intermediazione Finanziaria, 2015). Inoltre, questi dati sono stati anche confermati geograficamente dalla mappa d'incidenza regionale realizzata con QGIS, la quale ha rilevato come le regioni maggiormente colpite da reati informatici siano effettivamente quelle con un indice di vecchiaia più alto. Successivamente è stato mostrato come la percentuale di persone non accorte al tema della cyber prevenzione è proporzionale rispetto all'incremento nel numero di frodi su scala nazionale. Risulta inoltre importante sottolineare come i dati emersi tramite la seconda ipotesi sembrano trovare conferma anche in quella che viene definita da Burgard & Schemblach (2013) la 'prima fase' del processo di vittimizzazione informatica (cfr. p. 3).

Infine, è stato svelato come l'aumento della frequenza di acquisti online, coadiuvato anche dall'affermazione mondiale degli Smartphone e Tablet, risulta essere proporzionale rispetto alla crescita di frodi informatiche denunciate nell'ultimo triennio. A tale riguardo i dati delle ricerche sull'argomento hanno rilevato che si è raggiunto un significativo +21% di acquisti realizzati solo tramite Smartphone (Corriere Comunicazioni, 2016), il quale si accompagna in maniera piuttosto proporzionale al +23% di frodi informatiche registrate nell'ultimo triennio (quasi 1/1).

Pertanto, la conferma delle tre ipotesi apre un'importante parentesi esplorativa del fenomeno criminologico delle 'cyber frodi' in Italia. Infatti tale ricerca, nonostante si sia avvalsa di 'secondary data' (dati preesistenti), ha dimostrato l'esistenza di tre fattori molto importanti che potrebbero spiegare le cause alla base della natura endemica (e crescente) delle frodi online. Innanzitutto, si potrebbe affermare che l'età del cybernauta può avere un impatto sul rischio di vittimizzazione: più precisamente, l'inferenza che ne deriva è che date le minori competenze e conoscenze del mondo cibernetico da parte degli anziani (non essendo parte della 'generazione digitale') essi possano essere facili vittime di frodi online. Pertanto, in un'ottica preventiva, particolare attenzione dovrebbe essere data allo sviluppo di contromisure, metodologie o interventi che possano permettere una maggiore tutela di questa fascia di internauti più vulnerabile. Successivamente, questa ricerca ha rilevato come un altro fattore molto importante che potrebbe spiegare l'incremento di frodi negli ultimi anni è la mancanza di educazione ed attenzione ai pericoli dell'etere digitale da parte degli internauti stessi. Perciò, preventivamente parlando, un focus particolare dovrebbe essere rivolto ad opere di sensibilizzazione dei naviganti come ad esempio pubblicità sicure, notiziari oppure note informative provenienti sia da banche accreditate e sia da 'retailer' fidati in rete. Infine, è stato evidenziato come l'aumento della frequenza di acquisti online da un lato e il maggior acquisto di Smartphone dall'altro sia effettivamente proporzionale all'incremento di frodi negli ultimi anni potendo così affermare che la significativa crescita nelle vendite di questi prodotti non è stata accompagnata da un altrettanto significativa sensibilizzazione verso il più corretto utilizzo di questi strumenti. Pertanto, in un'ottica preventiva, potrebbe essere importante fornire al momento della vendita del prodotto cibernetico brochure informative che spieghino in via sintetica le principali minacce che potrebbero essere riscontrate nell'etere, così da favorire un'iniziale (seppure minimo) processo informativo del cliente e futuro internauta.

Infine, questi risultati, oltre a rivelare la prevalenza delle 'cyber frodi' sul territorio, hanno anche permesso una comprensione di alcune potenziali cause 'eziopatogenetiche' alla base di questo fenomeno endemico italiano. Infatti ha innanzitutto permesso di confermare quanto emerso dalle ricerche più recenti sull'argomento e cioè che il problema delle 'cyber frodi' è ben presente e diffuso a livello (inter)nazionale. Inoltre questo studio ha fornito un altro contributo importante. Infatti, ha esplorato il suddetto fenomeno attraverso l'uso di una prospettiva scientifica-sociale al contesto italiano che, come riportato da Holtfreter et al. (2008) e da Pratt et al. (2010), ha voluto riflettere sulle opportunità criminali offerte dal mondo digitale e come queste si vadano ad integrare coi fattori sociali-ambientali circostanti. In tal senso l'identificazione di tre potenziali fattori come l'indice di vecchiaia, la mancata attenzione alle misure protettive online ed il rapporto esistente fra la crescita numerica di frodi informatiche e la percentuale crescente di smartphone/tablet utilizzati forniscono un'importante linea guida per futuri studi esplorativi rivolti ad una maggiore prevenzione.

Riferimenti bibliografici

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., J., G., Levi, M., Moore, T. & Savage, S. (2012) *Measuring the cost of cybercrime. Workshop on the Economics of Information Security, Berlin, June 2012*. http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf, *accessed January 22, 2013*.

Associazione Bancaria Italiana (ABI) (2017). Nelle Banche Misure Efficaci Contro le Frodi Informatiche. Ottenuto da: http://www.abi.it/Pagine/news/Frodi-informatiche.aspx?showLogMask=on

Audiweb (2016). *Sintesi dei Dati 2016*. Retrieved Giugno, 2016, from http://www.audiweb.it/dati/disponibili-i-dati-audiweb-database-total-digital-audience-giugno-2016/

Baumeister, R., F. (2002).Yielding to temptation: Self-control failure, impulsive purchasing, and consumer behavior. *Journal of Consumer Research* , 28, 670-676.

Buizza, P. (2017). *Frode Informatica, 21 siti sequestrati*. Retrieved Agosto, 9, 2017 from http://www.bresciaoggi.it/territori/città/frode-informatica-21-siti-sequestrati-1.5886040

Burgard, A. & Schlembach, C. (2013). Frames of Fraud: a Qualitative Analysis of the Structure and Process of Victimization on the Internet. *International Journal of Cyber Criminology*, 7(2), 112-124.

Cancellato, F. (2014). *I Madoff italiani, è record di frodi finanziarie*. Retrieved Ottobre, 24, 2017 from http://www.linkiesta.it/it/article/2014/10/24/i-madoff-italiani-e-record-di-frodi-finanziarie/23261/

Chainey, S. (2014). *Hypothesis Testing Crime Analysis*. JDiBrief Series. London: UCL Jill Dando Institute of Security and Crime Science. ISSN: 2050-4853. Available from www.jdibrief.com

Corriere Comunicazioni (Cor.Com) (2015). *Frodi Online, in Italia manca l'educazione*. Retrieved Aprile, 26, 2015 from http://www.corrierecomunicazioni.it/it-world/33903_frodi-online-in-italia-manca-l-educazione.htm

Corriere Comunicazioni (Cor.Com) (2016). *E-Shopper in volata, in Italia sono 19 milioni*. Retrieved Maggio, 18, 2016 from http://www.corrierecomunicazioni.it/digital/41521_e-shopper-in-volata-in-italia-sono-19—milioni.htm

Centrale Rischi Finanziari (Crif) (2015). *Osservatorio Crif sui furti d'identità e le frodi creditizie in Italia*. Retrieved Dicembre, 2015 from https://www.crif.it/ricerche-e-pubblicazioni/osservatorio-sulle-frodi-creditizie/2015/dicembre/osservatorio-frodi-dicembre-2015/

Cultur-E (2017). *Il numero di anziani in rete cresce a ritmi elevati e, allo stesso tempo, crescono i rischi per i naviganti over 65*. Retrieved Giugno, 2016 from http://www.fastweb.it/web-e-digital/anziani-come-evitare-le-truffe-online/

Custodero, A. (2007). *Un reato su 3 commesso da immigrati*. Retrieved Maggio, 2007 from http://ricerca.repubblica.it/repubblica/archivio/repubblica/2007/05/10/un-reato-su-commesso-da-immigrati.html

Destri, F. (2017). *La frode informatica spaventa due aziende italiane su tre*. Retrieved Marzo, 10, 2017 from https://www.cwi.it/sicurezza/sicurezza-dei-dati/la-frode-informatica-aziende-italiane-103139

EL (2016). *Frodi Informatiche, il crimine cibernetico colpisce il 45% dei consumatori*. Retrieved Ottobre, 27, 2016 from http://www.helpconsumatori.it/primo-piano/frodi-informatiche-il-crimine-cibernetico-colpisce-il-45-dei-consumatori/108121

Florêncio, D., & Herley, C. (2013). Sex, lies and cyber-crime surveys. *Economics of information security and privacy III* (pp. 35–53). New York, NY: Springer. Retrieved from http://research.microsoft.com/pubs/149886/SexLiesandCybercrimeSurveys.pdf

Fortinet, G., L. (2009). *Fighting Cybercrime: technical, juridical, and ethical challenges*.Virus Bullettin Conference.

Freiermuth, M., R. (2011). Text, lies and electronic bait: An analysis of email fraud and the decisions of the unsuspecting. *Discourse & Communication*, 5(2), 123-145.

Gianotti, A. (2016). *Italia, più di 7500 reati al giorno. Scopri le provincie "criminali"*. Retrieved Ottobre, 3, 2016 from http://www.infodata.ilsole24ore.com/2016/10/03/18162/?refresh_ce=1

Giordano, M., T. (2015). *Le frodi man-in-the-middle, truffe informatico-finanziarie che provocano danni da migliaia di euro alle aziende*. Retrieved Giugno, 26, 2015 from http://www.repmag.it/rubriche/diritto-della-rete/item/282-le-frodi-man-in-the-middle-truffe-informatico-finanziarie-che-provocano-danni-da-migliaia-di-euro-alle-aziende.html

Goffman, E. (1974). *Frame Analysis: An Essay on the Organization of Experience*. Cambridge (MA): Harvard University Press.

Gross, M., L., Canetti, D. & Vashdi, D., R. (2016).The Psychological Effects of Cyber Terrorism. *Bulletin of the Atomic Scientist,* 72(5), 284-291.

Hassan, A., B., Lass, F, D. & Makinde, J. (2012). Cybercrime in Nigeria: causes, effects, and the way out. *Journal of Science and Technology*, 2(7), 626-631.

Holt, T. J., & Lampke, E. (2010). Exploring stolen data markets online: Products and market forces. *Criminal Justice Studies, 23*, 33–50.10.1080/14786011003634415

Holtfreter, K., Reisig, M., D. & Pratt, T., C. (2008). 'Low Self-control, Routine Activities, and Fraud Victimization. *Criminology*, 46, 189-220.

Idealo Magazine (2017). *e-Commerce in Italia: indagine sui consumatori digitali italiani*. Ottenuto da: https://www.idealo.it/magazine/-2017/01/10/e-commerce-in-italia-indagine-sui-consumatori-digitali-italiani/

Ionescu, L., Mirea, V. & Blajan, A. (2011). Fraud, Corruption and Cyber Crime in a Global Digital Network. *Economics, Management, and Financial Markets*, 6(2), 373-380.

Jaishankar, K. (2007). Establishing a Theory of Cyber Crimes. *International Journal of Cyber Criminology*, 1(2), 7-9.

Jaishankar, K. (2010).The Future of Cyber Criminology: Challenges and Opportunities. *International Journal of Cyber Criminology*, 4(1&2), 26-31.

Joseph, A., E. (2006). *Cybercrime Definition*. Retrieved, 2006 from http://www.crime-research.org/articles/joseph06/

Ministero degli Interni (2017). *Dati e Statistiche*. Retrieved, 2017 from http://www.interno.gov.it/it/sala-stampa/dati-e-statistiche

Njanike, K., Dube T. & Mashanyanye E. (2009). The Effectiveness of Forensic Auditing in Detecting, Investigating and Preventing Bank Frauds. *Journal of Sustainable Development in Africa*, 10(4), 405-425.

Osservatori.Net (2017). *Più del 60% del tempo speso dai consumatori online proviene dagli Smartphone*. Retrieved Febbraio, 9, 2017 from https://www.osservatori.net/it_it/osservatori/executive-briefing/piu-del-60-del-tempo-speso-dai-consumatori-online-proviene-da-smartphone

Perlroth, N. (2014). *Anonymous Hackers' efforts to identify Ferguson Police Officer Create Turmoil*. Retrieved Agosto, 14, 2014 from https://www.nytimes.com/2014/08/15/us/ferguson-case-roils-collective-called-anonymous.html

PLUS 24 Ore (2015). *Rischi noti ai più ma poche le difese*. Retrieved from https://www.crif.it/Media/Attachments/ 1431/PLUS_-11_10_14.pdf

Pratt, T., C., Holtfreter, K. & Reisig, M., D. (2010). Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory. *Journal of Research in Crime and Delinquency*, 47(3), 267-296.

PricewaterhouseCoopers (PWC) (2017). *Total Retail: la partita tra negozio e online in 10 mosse*. Retrieved, 2017 from https:/

/www.pwc.com/it/it/industries/retail-consumer/total-retail-2017/assets/docs/total-retail-2017.pdf

Rajasthan, A. (2013). An Investigative Study of Banking Cyber Frauds with special Reference to Private and Public Sector Banks. *Research Journal of Management Sciences*, 2(7), 22-27.

Rogers, A. (2014). *What Anonymous is Doing in Ferguson*. Retrieved, August, 21, 2014 from http://time.com/3148925/ferguson-michael-brown-anonymous/

UrbiStat (2017). *Classifica e Mappa Tematica dell'Indice di Vecchiaia in Italia*. Retrieved, 2017 from https://ugeo.urbistat.com/AdminStat

Williams, D.A. (2007). Credit Card Fraud in Trinidad and Tobago. *Journal of Financial Crime*, 14(3), 227-249.

Zunino, C. (2016). *Il Boom dello Smartphone e di Whatsapp. Censis: tre italiani su quattro viaggiano su internet*. Retrieved, Settembre, 28, 2016 from http://www.repubblica.it/cronaca/ 2016/-09/28/news/il_boom_dello_smartphone_e_di_whatsapp_censis_tre_italiani_siu_quattro_viaggiano_su_internet-148678843/?refresh_ce