# I quaderni di Agenda Digitale.eu

MAGGIO-AGOSTO 2024

n. 0017

Agendadigitale.eu è una testata scientifica e giornalistica registrata al Tribunale di Milano

**Dati di riferimento**

Iscrizione ROC n. 16446
ISSN 2421-4167
Numero registrazione 1927, Tribunale di Milano Editore:
Digital360

**Focus e ambito**

La rivista scientifica, i Quaderni di Agendadigitale.eu, pubblica fascicoli quadrimestrali in open access.

Lo scopo è creare un luogo per accompagnare i passi dell'Italia verso la necessaria rivoluzione digitale, con approfondimenti multidisciplinari a firma di esperti delle materie afferenti all'Agenda Digitale italiana ed europea

**Submission e norme editoriali**

Per effettuare una submission è necessario concordare prima un argomento e le misure precise contattando info@agendadigitale.eu.

Inviare un abstract di circa 500 caratteri alla testata, presentando l'articolo.

Le misure del testo finale saranno comprese tra 6mila e 20mila caratteri, salvo accordi per misure superiori.

I riferimenti bibliografici dovranno essere preparati in conformità alle regole dell'APA style, 6a edizione (si vedano le linee guida e il tutorial).

Gli autori sono invitati a tener conto degli articoli già pubblicati nella rivista e di citarli nel loro contributo qualora siano ritenuti di interesse per il tema trattato.

## Comitato editoriale

**Luca Toschi,** professore ordinario di Sociologia dei processi culturali e comunicativi presso l'Università di Firenze

## Comitato di referaggio

**Coordinatore: Luca Gastaldi, Polimi**

**Mauro Andreolini**, sicurezza informatica, Unimore
**Luca Baccaro**, concorrenza, diritto comunicazioni elettroniche e dei media; studio legale Lipani Catricalà & Partner
**Raffaello Balocco,** IT e innovazione, Politecnico di Milano
**Francesco Capparelli**, privacy, cyber security, ecommerce, data management, identità digitale; studio legale ICT Legal Consulting
**Antonio Chella,** ingegneria informatica, intelligenza artificiale, Università di Palermo
**Marco Centorrino**, Università di Messina – processi culturali e comunicativi, nuove tecnologie
**Ida Cortoni**, media education e digital literacy; Dipartimento di Comunicazione e Ricerca Sociale, Sapienza Università di Roma
**Giuseppe D'Acquisto**, Autorità garante privacy, sicurezza e privacy
**Mario dal Co,** Economista e manager, già direttore dell'Agenzia per l'innovazione
**Lelio Demichelis,** Università Insubria, sociologia, economia
**Francesco Di Giorgi**, diritto dell'informazione e della comunicazione, tutela dei consumatori, diritto delle comunicazioni elettroniche; Agcom
**Leonella Di Mauro**, data management, e-commerce, tutela del consumatore, diritto delle comunicazioni elettroniche; Agcom **Luisa Franchina,** cyber security, Hermes Bay
**Luca Gastaldi**: eGov, sanità, telecomunicazioni, procurement pubblico, design thinking, Smart Working, Politecnico di Milano
**Maurizio Gentile**, professore associato, Università di Roma LUMSA, didattica e pedagogia
**Antonio Ghezzi**: strategia, business model, startups, mobile, Politecnico di Milano
**Ugo Imbriglia,** sociologo
**Gevisa La Rocca, Università Kore di Enna**, piattaforme digitali, communication research, analisi qualitativa dei dati
**Nicola La Sala**, registro degli operatori della comunicazione, fattura elettronica, industria4.0, editoria, cittadinanza digitale; Agcom
**Emanuele Lettieri**, sanità Politecnico di Milano
**Maria Beatrice Ligorio**, psicologia, università di Bari

**Marika Macchi**, economia, Unifi

**Riccardo Mangiaracina**: fatturazione elettronica, eCommerce, logistica e trasporti, export, Politecnico di Milano

**Mirco Marchetti**, Sicurezza informatica, unimore

**Chiara Marzocchi**, economia, Università di Manchester

**Cristina Masella, Sanità**, Politecnico di Milano

**Carmelina Maurizio,** Dipartimento di Filosofia e Scienze dell'Educazione Università di Torino

**Stefano Moriggi,** scienze della comunicazione, filosofia, Bicocca di Milano

**Davide Mula**, sanità digitale, cyber security, privacy; Agcom

**Simone Mulargia**, internet and social media studies; Lumsa

**Antonella Napoli**, sociologia, media e comunicazione, giornalista

**Sebastiano Nucera,** Università di Messina, Media e Tecnologie Indossabili

**Achille Pierre Paliotta**, Social cybersecurity, disinformazione, tecnologie digitali, intelligenza artificiale, sociologia economica; INAPP

**Francesco Paoletti**, docente di organizzazione aziendale e gestione delle risorse umane, Università degli Studi di Milano-Bicocca

**Norberto Patrignani**, computer ethics, filosofia, Politecnico di Torino

**Dunia Pepe**, Inapp e Università Roma Tre, cultura e formazione digitale

**Alessio Plebe**, Università di Messina, Scienze cognitive, pedagogiche, psicologiche

**Francesco Pira,** Unime, comunicazione pubblica, le dinamiche social, le fake news e i processi di disinformazione

**Franco Pizzetti**, diritto, privacy, università di Torino

**Barbara Quacquarelli**, scienze umane e formazione, università Milano Bicocca

**Antonio Rafele,** Sociologia dei processi culturali e comunicativi, Unicusano

**Filippo Renga**: turismo digitale, smart agrifood, finance and banking, mobile, Politecnico di Milano

**Angelo Rovatti,** tutela del diritto d'autore, diritti connessi, Diritto dei media; Agcom

**Christian Ruggiero**, sociologia del giornalismo e comunicazione politica; Dipartimento di Comunicazione e Ricerca Sociale, Sapienza Università di Roma

**Franco Torcellan,** Associazione RED – Laboratorio di Ricerca Educativa e Didattica "Formare Trasformare Innovare"

**Angela Tumino**: Internet of Things, logistica e trasporti, smart city, Politecnico di Milano

**Simone Vannuccini**, economia, SPRU

**Francesco Varanini,** filosofia, formazione, università di Pisa

**Guido Vetere,** Università Sapienza di Roma, intelligenza artificiale, tecnologia

## INDICE DEL FASCICOLO

Solberg J., 2012, "Googling the Archive: Digital Tools and the Practice of History", in "Advances in the History of Rhetoric", n.15, pp. 53–76.

Tomasi F., 2021, "Organizzare la conoscenza: Digital Humanities e Web Semantico", Editrice Bibliografica, Milano.

Townsend R.B., 2010, "How Is New Media Reshaping the Work of Historians?", in "Perspectives on History", November, http://www.historians.org/publications-and-directories/perspectives-on-history/november-2010/how-is-new-media-reshaping-the-work-of-historians.

Turbanti S., 2018, "Strumenti di misurazione della ricerca: dai database citazionali alle metriche del web", Editrice bibliografica, Milano.
Weller T., 2013, "History in the Digital Age", Routledge, Abingdon.

# Processi di vittimizzazione e furto di identità digitale: rischi e contromisure

Il furto di identità digitale è un fenomeno in crescita che comporta gravi conseguenze per le vittime, spesso sottovalutate. Questo contributo offre un'analisi approfondita del fenomeno, esaminando rischi, conseguenze vittimologiche e possibili contromisure che individui e istituzioni possono adottare per contrastare tali attacchi e proteggere le informazioni sensibili

Di **Sandra Sicurella**, Professoressa associata in Sociologia della Devianza e del Mutamento Sociale, Dipartimento di Sociologia e Diritto dell'Economia, Università di Bologna e **Simone Tuzza**, PhD. in Criminologia è assegnista di ricerca presso il Dipartimento di Sociologia e Diritto dell'Economia dell'Università di Bologna

## Abstract

Il furto di identità digitale è volto a carpire informazioni sensibili per fini illeciti e costituisce un problema diffuso. Questo tipo di violazione, declinabile in forme differenti, implica processi di vittimizzazione, non sempre adeguatamente considerati. Con il presente contributo, dopo un inquadramento teorico del fenomeno, si procederà a un'analisi vittimologica sui rischi e sulle ripercussioni derivanti da tale esperienza e si individueranno le contromisure che soggetti e istituzioni possono attuare per fronteggiare gli attacchi e proteggere le informazioni.

# Introduzione

Negli ultimi anni, a causa di un utilizzo sempre maggiore di Internet e delle tecnologie digitali, il furto di identità[58] online è diventato un problema crescente e globale inerente alla acquisizione non autorizzata delle informazioni e dati personali di un individuo allo scopo di commettere frodi o altri illeciti (Tajpour & Zamani, 2021). Oggi l'espressione, furto di identità digitale, viene quindi utilizzata per «catalogare diversi reati che coinvolgono l'uso fraudolento delle informazioni personali di un individuo per scopi criminali e senza il loro consenso» (Reyns, 2013, p. 217). In altre parole, questo tipo di furto si riferisce al processo mediante il quale un individuo acquisisce e utilizza le informazioni personali di un'altra persona per scopi illegali, come aprire un conto bancario o richiedere un prestito Chawki, 2021; Williams, 2016; Hille, Walsh & Cleveland, 2015). Di conseguenza, in questo contributo, affronteremo le forme in cui si manifesta questo fenomeno e, da una prospettiva non solo criminologica ma anche vittimologica, presenteremo alcune delle possibili conseguenze per le vittime e, infine, cercheremo di comprendere come gli attori coinvolti, sia istituzionali sia privati, possono intervenire per contrastarne gli effetti. Più specificamente, nella prima parte, contestualizzeremo il fenomeno nella sua componente digitale, definiremo i confini del dibattito sulla distinzione tra frode e furto e analizzeremo i fattori di rischio associati. Successivamente, concentreremo la riflessione sulla dimensione vittimologica del problema e sulle conseguenze vissute dalle vittime e, infine, concluderemo esaminando le varie contromisure atte a mitigare queste azioni.

Saranno escluse da questo contributo forme illecite relative all'acquisizione dell'identità nel contesto più specifico dei rapporti interpersonali, che può essere anche riconducibile a diverse forme di maltrattamento nelle relazioni intime, dove il movente non è quello meramente economico, ma è determinato dalla volontà di infangare la reputazione della vittima, prevalentemente di genere femminile (Stojakovic *et al.*, 2023). Furti di identità commessi al fine di diffamare, calunniare, screditare e rovinare la reputazione di una persona possono implicare conseguenze di diverso profilo perché la vittima, nella maggior parte dei casi, conosce l'autore e decide di non rivolgersi alle autorità oppure ritira una precedente denuncia. La bassa incidenza di denunce o segnalazioni di tali casi potrebbe essere imputabile ad una mancanza di fiducia nel sistema e potrebbe pertanto implicare una sottostima dei dati reali (CSD, 2022).

# Furto d'identità digitale: contesto e fattori di rischio

Lo spazio digitale offre notevoli vantaggi agli utenti che lo utilizzano, consentendo loro di beneficiare di informazioni, servizi e facilitazioni di vario genere. Tuttavia, allo stesso tempo, l'espansione di questo spazio digitale e l'interferenza, consapevole o meno, nella vita privata dei cittadini comportano un innegabile aumento della vulnerabilità e dei rischi che si possono incontrare. Come afferma Clarke (2004): « The Internet has created a completely new environment in which traditional crimes – fraud, identity theft and child pornography – can take new forms and thrive (p. 45). Fonti di danno includono il furto di identità digitale, che, negli ultimi tempi, ha visto non solo un aumento nella frequenza degli incidenti e, quindi, anche del numero delle vittime, ma anche la crescita di un particolare interesse all'interno della letteratura socio-criminologica, mirato ad analizzare l'incidenza degli incidenti, i

[58] Tuttavia, a questo proposito, è bene precisare che alcuni autori sono critici nei confronti della definizione di "identità" in relazione a questo fenomeno. Per esempio, Eve (2016) spiega che il concetto di identità è più legato al binomio conoscenza/potere piuttosto che alla designazione di un individuo. L'autore, quindi, sottolinea che esiste una «retorica del furto di identità» nel caso delle password, perché questi dati riservati vengono erroneamente considerati come una descrizione fedele di una persona, ma così non è perché: «[L]'identità che potremmo derivare da un sistema di password non è identica a una persona e non può esserlo» (Eve, 2016, p. 95).

fattori di rischio, gli elementi situazionali e le variabili protettive che possono influenzare il rischio di vittimizzazione.
Da un punto di vista criminologico, il furto di identità può essere inteso come un insieme di reati commessi in tre diverse fasi. Nella prima, l'offender può carpire le informazioni attraverso tecniche online, quali *haking*, *phishing*, *skimming*, o tecniche offline, come l'appropriazione fisica di documenti; la seconda fase può essere considerata come una fase intermedia durante la quale, prima dell'effettivo utilizzo a scopi criminali, le informazioni possono essere vendute su forum o specifici mercati online (*surface* e *dark web*); la terza, infine, riguarda l'uso delle informazioni relative all'identità rubata per la commissione di reati, quali per esempio frode con carta di credito (CSD, 2022). Questa sequenza di fasi suggerisce la complessità di un fenomeno che è in continuo aumento e che, al contempo, implica ingenti costi non solo di natura economica.
È quindi necessario porre l'attenzione alle nuove abitudini dei singoli, considerando anche la notevole diffusione delle transazioni senza contanti, che aumentano le probabilità di incorrere in episodi di vittimizzazione (Golladay & Holtfreter, 2017). Pertanto, è consigliabile iniziare a delineare e distinguere cosa si intende specificamente quando si parla di furto di identità digitale. Secondo alcuni autori (Button 2019; Collins, 2005) è importante distinguere il furto d'identità dalla frode, quest'ultima considerata in termini più generici, diversamente dal furto, che ha un aspetto di vittimizzazione più distintivo:

«Identity theft and identity fraud are terms that are often used interchangeably. Identity fraud is the umbrella term that refers to a number of crimes involving the use of false identification – though not necessarily a means of identification belonging to another person. Identity theft is the specific form of identity fraud that involves using the personally identifiable information of someone else. Both identity fraud and identity theft are crimes often committed in connection with other violations, as mentioned above. Identity theft, however, may involve an added element of victimisation, as this form of fraud may directly affect the life of the victim whose identity was stolen in addition to defrauding third parties[59]» (Finklea, 2014, p.78-79).

Nel 2019, uno studio, intitolato *"Risks and Societal Implications of Identity Theft"* (Kalvet, Tiits *et al.*, 2019), ha esaminato gli aspetti sociali del furto di identità online e ha suggerito che l'uso delle piattaforme di social media potrebbe aumentare il rischio di incappare in furti di questo tipo. La ricerca ha anche evidenziato la necessità di acquisire una maggiore consapevolezza e di ricevere un'educazione mirata rispetto alle abitudini sul web al fine di prevenire furti di identità. Nello stesso anno, un'altra ricerca (Ali *et al.*, 2019) ha analizzato le tecniche utilizzate dai truffatori per ottenere informazioni personali e finanziarie dai consumatori, giungendo a fornire suggerimenti per prevenire le frodi online. Questo studio ha quindi identificato alcuni dei metodi più comuni utilizzati dai trasgressori, come l'invio di e-mail di phishing[60], la creazione di siti web fraudolenti e l'uso di malware, vale a dire software dannosi in grado di compromettere qualsiasi tipo di dispositivo.
Infine, lo studio *"A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments"* (Li & Liu, 2021) ha esplorato le sfide legali e normative nella lotta al furto di identità online. Ha evidenziato, infatti, la necessità di una maggiore cooperazione tra le forze dell'ordine e le aziende tecnologiche per prevenire e combattere questo tipo di furto.

[59] https://digital.library.unt.edu/ark:/67531/metadc462892 , ultimo accesso 23 maggio 2023).
[60] Il phishing è un tipo di furto di identità online in cui gli aggressori utilizzano tattiche di ingegneria sociale per ingannare le persone e indurle a fornire le proprie informazioni personali, come nomi utente, password e informazioni sulle carte di credito. Gli attacchi di phishing possono essere effettuati tramite vari mezzi, tra cui e-mail, messaggi di testo e messaggi sui social media. Secondo uno studio del gruppo di lavoro anti-phishing (APWG), sono stati riportati oltre 1.122.579 attacchi di phishing unici dal 1° maggio 2021 al 30 aprile 2022. Per ulteriori dettagli: [https://apwg.org](https://apwg.org).

La produzione scientifica sul tema è molto vasta e gli studi sull'argomento spaziano con focus diversi e approfondimenti sui vari aspetti del fenomeno. Tra questi, una prima distinzione da tenere presente è relativa al fatto che il furto di identità può assumere diverse forme, tra le quali possiamo annoverare la dimensione finanziaria, concernente il tipo più comune di furto di identità, che comporta la sottrazione di informazioni finanziarie come dettagli delle carte di credito o dei conti bancari e può essere utilizzato per effettuare acquisti fraudolenti o prelevare denaro dal conto corrente della vittima (Van Der Meulen, 2011); la dimensione medico-sanitaria, che invece implica l'appropriazione di informazioni quali i dettagli dell'assicurazione sanitaria, che possono essere utilizzati per ottenere trattamenti medici o prescrizioni di farmaci a nome della vittima (Graham & Brown, 2011); la dimensione criminale, che comporta l'uso dell'identità di un'altra persona per commettere un crimine, come usare una patente di guida rubata per creare una falsa identità e, infine, la dimensione "sintetica" (*syntetic fraud*). In quest'ultimo caso il riferimento è alla creazione di una nuova identità, utilizzando una combinazione di informazioni personali reali e false. Questo tipo di furto di identità è particolarmente difficile da rilevare e prevenire[61].

Relativamente a queste macroaree, che designano il quadro del furto di identità, ci sono altrettanti fattori di rischio. È importante sottolineare che, nella maggior parte dei casi, i rischi ricadono sull'utente individuale, la cui condotta viene ritenuta "responsabile" quando diventa vittima. Tra i vari comportamenti individuali, è importante ricordare che l'uso di password deboli o il riutilizzo della stessa su più account può facilitare l'accesso dei ladri di identità a informazioni sensibili (Tajpour & Zamani, 2021). Inoltre, le reti Wi-Fi pubbliche e i siti web non sicuri possono offrire un facile punto d'ingresso ai truffatori[62]. Le truffe di phishing, che coinvolgono e-mail o siti web fraudolenti e ingannano gli utenti inducendoli a fornire informazioni personali, possono sfociare in furto d'identità se le persone cadono in queste trappole[63] così come la condivisione di informazioni personali online o con sconosciuti può aumentarne il rischio *(Ibidem).* Infine, le violazioni degli archivi di dati personali, che coinvolgono aziende o organizzazioni, possono esporre più facilmente gli individui al furto d'identità (Schlackl *et al.*, 2022).

È opportuno qui precisare che, più recentemente, si è compreso che focalizzarsi solo sugli utenti e non considerare coloro che sono responsabili della protezione dei dati personali è insufficiente per ottenere una comprensione completa del problema del furto d'identità. A questo proposito, infatti, l'*accountability* aziendale gioca un ruolo cruciale nell'affrontare il furto d'identità. Le aziende che raccolgono e archiviano informazioni personali hanno il dovere di proteggerle dall'accesso, dall'uso o dalla divulgazione non autorizzati. Se non riescono a tutelarle adeguatamente, possono causare gravi danni agli individui, inclusi perdite finanziarie e danni alla loro reputazione. Diversi studi sottolineano l'importanza della responsabilità aziendale nel prevenire il furto d'identità, proteggendo i dati personali e fornendo indicazioni alle aziende su come adempiere a questa responsabilità.

## Vittimizzazione e furto d'identità digitale: le esperienze delle vittime

Da un punto di vista vittimologico, ci sono diversi aspetti da analizzare per comprendere appieno le connotazioni specifiche di questo fenomeno. Implicazioni importanti, successive al processo di vittimizzazione determinato dal furto di identità, vengono spesso sottovalutate. Contrariamente a quanto comunemente ritenuto, le conseguenze possono avere pesanti ricadute sui soggetti che

[61] https://www.forbes.com/advisor/credit-score/what-is-synthetic-fraud/
[62] U.S. Federal Trade Commission, 2020.
[63] U.S. Department of Justice, 2019.

subiscono questo tipo di furto. Inoltre, da una parte, vengono sottovalutati gli aspetti emotivi e le ripercussioni sulle abitudini quotidiane e, dall'altra, non di rado le vittime vengono colpevolizzate per quello che viene ritenuto un comportamento imprudente o, peggio ancora, una leggerezza dettata dall'ingenuità.

A tal proposito, un recente studio di Reynolds (2023) evidenzia che, oltre alle perdite di tempo e denaro, coloro che subiscono un furto di identità possono altresì sviluppare difficoltà emotive, problemi di natura fisica e avere implicazioni anche dal punto di vista relazionale.

Un interessante studio sul furto di identità online (2022), condotto da ICF in collaborazione con CSD[64], Università di Trento e Victim Support Europe, consente di comprenderne le implicazioni sociali e normative, valutare l'entità, stimare il numero di vittime e le perdite economiche e conoscere le organizzazioni criminali maggiormente coinvolte.

In sintesi, la ricerca mette in evidenza come il furto d'identità costituisca una preoccupazione persistente dei cittadini europei.

Prendendo in esame i principali risultati e concentrando l'attenzione sulla prima sezione[65] inerente all'entità del furto di identità, maggiormente rilevante ai fini di questa analisi, apprendiamo che il *phishing* è la tecnica maggiormente usata per carpire dati personali (CDS, 2022). I reati sono commessi prevalentemente a scopo di lucro da gruppi, con caratteristiche organizzative più o meno strutturate di diverso tipo, provenienti dall'Europa, ma anche da Paesi non europei, associazioni internazionali che utilizzano metodi e strumenti di anonimizzazione di diversa natura, che rendono quindi più difficile individuare e perseguire i responsabili.

Nonostante un profilo delle vittime, tradizionalmente tracciato dalle precedenti ricerche, in relazione a dati demografici, personalità e, addirittura, in alcuni casi, tratti neurologici e inerente a fattori protettivi derivanti da esperienza e consapevolezza rispetto al problema o riluttanza alla condivisione online dei dati, i risultati di questa rilevazione sottolineano che chiunque può diventare una vittima del furto di identità online, anche se un accento va posto sulle categorie dei giovani, a causa di un maggiore utilizzo della tecnologia, e sugli anziani, al contrario, meno avvezzi alle nuove tecnologie.

I dati, ottenuti attraverso tecniche di *hacking* o acquistati sul *dark web*[66], sono utilizzati in modo prevalente per fini di lucro ai danni di privati (92%) e aziende[67] (77%) e sono di natura finanziaria, come per esempio quelli relativi alle carte di credito (CSD, 2022).

Per quanto concerne la stima di vittime, gli Autori ritengono che, nonostante i limiti, la fonte più completa da utilizzare sia the 2017-2019 Eurobarometer study, che mostra livelli più elevati di

[64] ICF, Inner City Fund., is a leading public policy research consultancy (https://www.icf.com) CSD: Center for the Study of Democracy (https://csd.bg)

[65] In the second section of work, you can find: "Section 2.1: The scale of identity theft describes the nature of the identity theft problem and provides an assessment of the scale of identity theft and related crimes, as well as cost estimates; Section 2.2: Mapping of relevant legislation across the EU – provides an overview of relevant legislation across the EU, first explaining the concept of identity theft and then looking more closely at Member States' approaches, including regulatory, procedural and operational gaps; Section 2.3: Mapping of relevant practical measures – provides an overview of the existing national regulatory and non-regulatory initiatives (strategies, policies), as well as Member States' practical measures and practices to prevent and combat online identity theft, mitigate the risk for consumers, and provide support to victims" (CDS, 2022, p. 14).

[66] Nell'aprile del 2023, un'importante operazione internazionale ha portato allo smantellamento e al sequestro di Genesis Market, uno dei più pericolosi market place che vendeva credenziali di account rubate agli hacker di tutto il mondo. Secondo Europol "Genesis Market was considered one of the biggest criminal facilitators, with over 1.5 million bot listings totalling over 2 million identities at the time of its takedown". https://www.europol.europa.eu

[67] Anche le aziende naturalmente possono subire attacchi e conseguenze serie non solo di natura finanziaria ma anche di credibilità per esempio. Tuttavia, in questo contributo si è scelto di incentrare l'analisi sulle persone, sugli utenti della rete.

vittimizzazione per furto di identità nei paesi Ue a più alto reddito, dato probabilmente da imputare a un uso maggiore da parte della popolazione di servizi online e online banking. Il phishing è il tipo di reato più diffuso seguito dall'installazione di software dannosi.
Sulla base dei dati di Eurobarometer, le stime del numero di vittime coprono un range, a seconda dei tipi di reato considerati, che oscilla tra i 19 e i 113 milioni (CSD, 2022).
Se, come abbiamo visto, nell'ambito della letteratura socio-criminologica, si è registrata una progressiva e crescente attenzione agli aspetti e alle caratteristiche del furto di identità digitale non possiamo affermare lo stesso a proposito dell'esperienza di vittimizzazione, che non ha ottenuto il medesimo riscontro in letteratura (Golladay, Holtfreter, 2016).
Molto spesso tale esperienza viene ricondotta a una mera perdita finanziaria, importante sì, ma non tale da determinare un cambiamento nelle abitudini di vita oppure conseguenze rilevanti di diversa natura.
Pochi studi hanno posto al centro della loro riflessione gli effetti derivanti dal processo di vittimizzazione subito. Tra questi, Randa e Reyns (2019) si soffermano ad analizzare le conseguenze emotive e fisiche successive all'esperienza di vittimizzazione. Lo studio, basandosi su un campione preesistente, derivante dalla U.S. National Crime Victimization Survey (2012), analizza i dati raccolti, giungendo a risultati interessanti. L'obiettivo della ricerca è, infatti, quello di rispondere ad alcune questioni, rilevanti in ambito criminologico, rispetto alla vittimizzazione derivante dal furto di identità. In particolare, gli Autori intendono analizzare gli effetti della vittimizzazione, causata dal furto d'identità.
Al di là delle conseguenze di natura finanziaria, le vittime denunciano disturbi fisici (problemi di sonno, stanchezza, disturbi allo stomaco, ecc.) e di carattere emotivo (preoccupazione/ansia, vulnerabilità, mancanza di fiducia nelle persone, ecc.) e ciò suggerisce che l'impatto sulle vittime è simile a quello determinato da altri tipi di reato; inoltre, dai risultati raggiunti, anche i fattori demografici e situazionali sembrano correlati in modo significativo agli effetti negativi sperimentati dalle vittime; infine, valutando anche esperienze ripetute di vittimizzazione, gli Autori ribadiscono l'importanza di identificare e prevenire vittimizzazioni ripetute, che determinano una ulteriore sofferenza per le vittime (Randa, Reyns, 2019).
Qualche anno prima, nel 2016, sulla stessa linea d'onda, le ricercatrici Golladay e Holtfreter, che ritengono poco indagate empiricamente le conseguenze derivanti dal processo di vittimizzazione successivo al furto di identità, analizzano le conseguenze di natura fisica ed emotiva di tale reato al fine di sopperire alle lacune in letteratura, molto più spesso orientata alle conseguenze vittimologiche dei crimini violenti (Golladay e Holtfreter, 2016).
Le autrici prendono in considerazione il rischio di vittimizzazione in relazione alle caratteristiche demografiche, riscontrando una maggiore incidenza del fenomeno nella fascia d'età tra 25 e 64 anni, età dopo la quale il fenomeno sembra decrescere e nessuna sostanziale differenza tra uomini e donne. Altri elementi da considerare, in questa analisi, attengono allo stato civile, al reddito, alla ubicazione geografica e al numero di figli. Un maggior numero di figli e un reddito più elevato, per esempio, dovrebbero implicare un maggiore rischio di vittimizzazione.
Alcuni studi ancora precedenti (Sharp *et al.*, 2004; ITCR, 2014), basati su un campione complessivo di 238 vittime di furto di identità, possono essere citati a supporto dell'ipotesi che tali vittime, oltre alle perdite finanziarie, sperimentino conseguenze di natura emotiva e fisica. È un apporto, tuttavia, che non si fonda su campioni significativi (Golladay e Holtfreter, 2016).
Pur avvalendosi dei medesimi dati dello studio di Randa e Reyns, the researchers utilizzano un approccio teorico differente, fornendo un supporto empirico alla General Strain Theory di Agnew perché «(…) la vittimizzazione del furto di identità può essere concepita come un fattore di stress che

si traduce in una serie di emozioni negative come depressione e ansia» (Golladay e Holtfreter, 2016, pp. 15-16). Lo studio di Golladay e Holtfreter è uno dei pochi che si interroga sul danno occorso alla vittima di furto di identità e sottolinea che, sebbene tale reato spesso non sia considerato per gravità alla stessa stregua di altri, il livello e il tipo di conseguenze patite dalle vittime suggeriscono un orientamento diverso perché, al di là dei danni finanziari, può causare una sintomatologia emotiva e fisica, che si protrae oltre l'evento stesso (Golladay e Holtfreter, 2016).

Rispetto alla situazione che precede la vittimizzazione, della quale si conosce poco, Norah Ylang applica il concetto di "guardianship", tratto dalla nota teoria di Cohen e Felson (1979), all'uso di misure di autoprotezione in una popolazione generale con l'obiettivo di esaminare i fattori demografici degli individui che adottano misure per proteggersi dalla vittimizzazione del furto d'identità (Ylang, 2020). L'Autrice sostiene che, sebbene la responsabilità della prevenzione rispetto al furto di identità non sia da attribuire esclusivamente agli utenti, ma riguardi anche le organizzazioni (comprese le aziende e i governi) che raccolgono e utilizzano le loro informazioni e gli organi legislativi, che regolano il trattamento delle informazioni personali, il ruolo degli utenti resta cruciale perché la disattenzione può vanificare il lavoro di prevenzione svolto da governi e aziende (Ylang, 2020).

Incrociando i dati demografici (età, sesso, istruzione, stato civile e reddito) con la variabile dipendente, *capable guardianship* (Cohen, Felson, 1979), Ylang afferma che «Based on the findings, these individuals are much more likely to be white, female and more educated. Annual income exerted far less direct influence over the exercising of capable guardianship» (Ylang, 2020, p. 139).

Secondo questo studio, pertanto, le caratteristiche demografiche incidono sulle misure di autoprotezione che vengono adottate e, sebbene non privo di limiti, suggerisce l'importanza di misure proattive da parte degli utenti al fine di prevenire o minimizzare i danni del furto di identità (Ylang, 2020). Ciononostante, è importante riuscire a bilanciare correttamente i fattori di rischio e le eventuali caratteristiche delle vittime onde evitare di incappare in un processo di colpevolizzazione della vittima.

Spesso, infatti, viene attribuita la responsabilità ai singoli e a focalizzare l'attenzione sul ruolo dell'individuo piuttosto che chiamare in causa soluzioni strutturali di polizia o politiche. Sembra, in alcuni casi, presente una maggiore attenzione alle azioni e alle strategie che il singolo deve adottare al fine di proteggersi piuttosto che una riflessione sul ruolo che le aziende e gli stessi governi assumono in tale contesto. Emergono inoltre alcune contraddizioni in seno alle stesse istituzione che che, da un lato, evidenziano l'opportunità di misure appropriate atte a prevenire il furto di identità e la conseguente vittimizzazione e, dall'altro, lo descrivono come inevitabile anche di fronte a strategie preventive adeguate (Reynolds, 2023).

Dalla ricerca, realizzata da Reynolds (2023), emergono due temi contrastanti che vedono il furto di identità, da una parte, come inevitabile e, dall'altra, dovuto a vittime ingenue, non esperte di tecnologia, anziane o comunque colpevoli. Si evidenziano quindi alcuni nodi centrali come l'inevitabilità e una descrizione stereotipata della vittima cui si sommano atteggiamenti di colpevolizzazione e di autocolpevolizzazione. Quest'ultimo aspetto comporta particolari resistenze rispetto alla scelta di denunciare o, più semplicemente di raccontare l'accaduto anche se a familiari o amici e pertanto l'imbarazzo e la vergogna per non essere stati in grado di autoproteggersi frenano e costituiscono un ostacolo nella ricerca di aiuto. Le vittime subiscono un processo di *victim blaming*, viene riconosciuto loro un ruolo attivo senza tenere conto della sofisticazione degli strumenti e delle tecniche avanzate utilizzate dai ladri di identità digitali (Drew e Cross, 2013).

Per attenuare questi effetti, così come suggerito da Cole e Pontell (2006), i governi potrebbero fare pressione sulle istituzioni, che raccolgono e detengono informazioni personali per implementare misure di sicurezza più rigorose al fine di proteggere meglio i cittadini.

## Contromisure

Esulando da caratteristiche personali specifiche, che potrebbero distorcere le attribuzioni di responsabilità a svantaggio delle vittime, le aziende responsabili della gestione e della protezione dei dati sensibili dei clienti possono implementare diverse strategie per prevenire e tutelare queste informazioni. Nel complesso, le aziende devono prioritariamente salvaguardare i dati e adottare misure adeguate a prevenire il furto di identità. Questo non solo aiuta a tutelare le persone, ma contribuisce anche a stabilire rapporti di fiducia con i clienti (Maitlo, 2019; Sullins, 2006) e gli stakeholder, il che è essenziale per il successo a lungo termine.

In relazione al furto di identità, le aziende, infatti, possono adoperarsi per garantire una protezione maggiore e a più livelli. In particolare, dovrebbero adottare misure adeguate a proteggersi da violazioni riguardati i dati, come l'implementazione di controlli di accesso, la crittografia delle informazioni sensibili e la regolare verifica dei loro sistemi per individuare eventuali vulnerabilità (Murdoch, 2021). Inoltre, esse devono garantire trasparenza riguardo alle informazioni personali che raccolgono e utilizzano. Ciò significa non solo fornire politiche sulla *privacy* chiare e concise, ma anche ottenere il consenso prima di chiedere e adoperare le informazioni personali. È altresì importante notificare tempestivamente la violazione dei sistemi di protezione dei dati in modo tale da consentire di adottare misure appropriate per proteggersi come, per esempio, l'aggiornamento delle proprie password. Responsabilità e collaborazione, infine, possono rappresentare due parole chiave atte a delineare la posizione delle aziende in questo delicato equilibrio di raccolta sistematica e gestione di informazioni. Esse, infatti, non solo devono essere ritenute responsabili delle loro azioni ma, più precisamente, devono assumersi l'onere di eventuali violazioni di dati e compensare gli individui che hanno subito danni a seguito della violazione stessa. Devono altresì collaborare con i governi e altri stakeholder per sviluppare e implementare le migliori pratiche per la protezione dei dati e la prevenzione del furto di identità[68].

Inoltre, insieme ai governi che devono tutelare i loro cittadini in un mondo sempre più globale e interconnesso, le aziende e le istituzioni possono proporre politiche comuni per impedire, o quanto meno ridurre, il furto di identità.

In questa direzione e prendendo ad esempio il Regolamento generale sulla protezione dei dati (GDPR) europeo[69], i governi possono proporre leggi più stringenti sulla protezione dei dati, regolandone la raccolta, la conservazione e l'utilizzo da parte delle aziende, nonché richiedendo alle aziende di notificare tempestivamente ai consumatori le avvenute violazioni dei dati e la necessità di adottare misure appropriate per proteggere le loro informazioni personali. In secondo luogo, prendendo spunto dalla direttiva europea 2022/2555[70] – entrata in vigore nel 2023 – le aziende possono migliorare le loro misure di sicurezza informatica per proteggersi dagli attacchi informatici. Questo include il rafforzamento dei controlli di accesso, la crittografia dei dati sensibili e la verifica regolare dei sistemi per individuare precocemente potenziali vulnerabilità. In questo modo, governi e aziende possono adottare misure per proteggere le infrastrutture critiche, come reti di telecomunicazioni e impianti di produzione di energia, da attacchi informatici e tentativi di furto di dati sensibili.

[68] "Corporate Identity Theft Prevention and Response: A Best Practices Guide" by the Identity Theft Prevention and Identity Management Standards Panel (IDSP) (2019).

[69] Regulation (2016/679) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/Ec (Data Protection Directive).

[70] Directive (EU) 2022/2555 of the European Parliament and of the council on measures for a high common level of cybersecurity across the union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

Infatti, secondo questa direttiva più recente, le aziende identificate come gestori di servizi essenziali, come energia, trasporti, acqua, infrastrutture bancarie, mercati finanziari, assistenza sanitaria e infrastrutture digitali, devono implementare adeguate misure di sicurezza e segnalare incidenti gravi alle autorità nazionali competenti. I principali fornitori di servizi digitali, come motori di ricerca, servizi di *cloud computing* e *marketplace online*, devono conformarsi ai requisiti di sicurezza e notifica indicati nella direttiva. Infine, è fondamentale che i vari attori privati e pubblici coinvolti forniscano informazioni chiare sulla privacy: governi e aziende possono condividere indicazioni chiare e trasparenti sulla raccolta, l'uso e la condivisione dei dati personali degli utenti[71], in modo che i cittadini siano consapevoli dei rischi e delle protezioni a loro disposizione.
A questo proposito, una maggiore formazione sull'argomento è essenziale. Governi e aziende possono, infatti, educare gli utenti su come proteggere le proprie informazioni personali online e questo, quindi, include suggerimenti sulla creazione di password più difficili da decodificare, istruzioni atte a riconoscere tentativi di phishing e consigli sull'inopportuna abitudine di condividere sul web informazioni personali[72]. Quando invece il danno è già stato determinato da condotte illecite, le vittime devono essere seguite e compensate sia dalle autorità sia dalle aziende per rispondere ai significativi disagi finanziari ed emotivi che ne conseguono.
È quindi evidente che, per mettere in atto contromisure efficaci contro il furto di identità online, è necessaria una sinergia che coinvolga a diversi livelli governi, aziende e utenti. Solo con uno sforzo congiunto dal basso verso l'alto sarà possibile attuare strategie capaci di contrastare le varie dimensioni di un fenomeno in crescita come il furto di identità.

# Conclusioni

Questo contributo presenta una panoramica – sebbene non esaustiva – delle varie tipologie, dinamiche e dimensioni sociali legate al furto di identità online. Inizialmente è stata fornita una definizione teorica del fenomeno, successivamente, il contributo si è concentrato sul furto di identità, le frodi e le caratteristiche a livello digitale, come quelle relative ai dati sensibili o alle perdite finanziarie correlate. Inoltre, si è tentato di evidenziare i vari fattori di rischio e le contromisure che possono essere messe in atto a diversi livelli: sia da parte degli utenti, ma soprattutto dalle aziende e dai governi coinvolti, i quali devono proteggere i dati e garantire i diritti delle vittime. A questo proposito, vale la pena sottolineare – ancora una volta – come eventuali responsabilità individuali non dovrebbero assolvere le istituzioni incaricate di tutelare i cittadini. Un importante studio di Reynolds (2023), infatti, mette in luce come i messaggi istituzionali sulla responsabilità individuale degli utenti di fronte al furto di identità in realtà mascherino una deresponsabilizzazione delle istituzioni e finiscano sostanzialmente per influenzare negativamente la richiesta di aiuto e di denuncia delle vittime. Queste ultime, contrariamente a quanto comunemente ritenuto, non subiscono soltanto perdite economiche, ma conseguenze di varia natura da imputare anche a un contesto sociale, che spesso le colpevolizza per ciò che hanno subito. Per dare luce a questi aspetti, che non sempre trovano adeguata collocazione in letteratura, si è scelto di procedere all'analisi del fenomeno attraverso un approccio vittimologico, che tenga conto dei vari aspetti che concorrono a definire l'esperienza vittimizzante. L'obiettivo ultimo di questa panoramica è fornire al lettore alcuni strumenti interpretativi per comprendere maggiormente

[71] Data Protection in the European Union: The Role of National Law and the European Union, 2019.
[72] Esistono diverse strategie che gli utenti possono adottare per difendersi dal furto di identità online. Ad esempio, è essenziale utilizzare password robuste e uniche per ogni account online. Evitare di utilizzare la stessa password per più account e usare una combinazione di lettere, numeri e simboli per rendere le password difficili da indovinare.

il furto di identità digitale che, a prescindere dalle diverse modalità di sottrazione e successiva appropriazione di dati e informazioni, si presenta come un fenomeno complesso in grado di coinvolgere attori diversi, dai singoli utenti alle istituzioni e dalle forze di polizia alle aziende.

# Bibliografia


Ali, M. A. Azad, M. Parreno Centeno, F. Hao and A. van Moorsel, (2019), "Consumer-facing technology fraud: Economics, attack methods and potential solutions", Future Generation Computer Systems 100, pp. 408-427.

Button, M. (2019). Digital Fraud: Preventing, Investigating and Responding, Journal of Financial Crime, Volume: 26, Numero 2, p. 423-431, DOI: 10.1108/JFC-11-2017-0111.

Chawki, M. (2021), "Cybercrime in the Context of COVID-19," in K. Arai (ed.), Intelligent Computing. Lecture Notes in Networks and Systems, vol. 285. Cham, Springer, 2021.

Clarke, R.V. (2004), "Technology, Criminology and Crime Science", European Journal on Criminal Policy and Research 10.

Cohen, L. and Felson, M. (1979), "Social change and crime rate trends: a routine activity approach", American Sociological Review, Vol. 52 No. 2, pp. 170-183.

Cole SA and Pontell HN (2006) 'Don't be low hanging fruit': Identity theft as moral panic. In: Monahan T (ed.) Surveillance and Security: Technological Politics and Power in Everyday Life. New York: Rout- ledge, pp. 125–147.

Collins, J. M. (2005), Preventing Identity Theft in Your Business: How to Protect Your Business, Customers, and Employees, Wiley.

CSD. Study on online identity theft and identity-related crime. Sofia: CSD, 2022

Drew JM and Cross C (2013) Fraud and its PREY: Conceptualising social engineering tactics and its impact on financial literacy outcomes. Journal of Financial Services Marketing 18(3): 188–198.

European Commission, Directorate-General for Migration and Home Affairs, Study on online identity theft and identity-related crime: final report, Publications Office of the European Union, 2022, https://data.europa.eu/doi/10.2837/197724

Eve, M.P. (2016), Password, New York, Bloomsbury Academic,

Finklea, K. (2014) Identity Theft: Trends and Issues, Report, 16 January 2014; Washington D.C., pp. 78-79, (https://digital.library.unt.edu/ark:/67531/metadc462892, accessed 23 May 2023).

Golladay K., Holtfreter, K. (2017),"The Consequences of Identity Theft Victimization: An Examination of Emotional and Physical Health Outcomes," 2017 Victims & Offenders 12:5, 741-760.

Graham, J., Brown S., (2011), "Medical Identity Theft: The Future Threat of Health Care Fraud in America", 2011 FBI Law Enforcement Bulletin 80(11), 1-8.

Katelyn Golladay & Kristy Holtfreter (2016): The Consequences of Identity Theft Victimization: An Examination of Emotional and Physical Health Outcomes, Victims &Offenders.

Kalvet T., Tiits M., Ubakivi-Hadachi, P. (2018) "Risks and Societal Implications of Identity Theft," in A. Chugunov, Y. Misnikov, E. Roshchin and D. Trutnev (eds), Electronic Governance and Open Society: Challenges in Eurasia, Series "Communications in Computer and Information Science," vol. 947, Cham, Springer, 2018.

Hille, G. Walsh and M. Cleveland, "Consumer Fear of Online Identity Theft: Scale Development and Validation," 2015 Journal of Interactive Marketing 30(1), 1-19.

Li, Y., Liu, Q. (2021) "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," 2021 Energy Reports 7, pp. 8176-8186.

Maitlo, A. (2019), "Preventing Identity Theft: Identifying Major Barriers to Knowledge-sharing in Online Retail Organisations," 2019 Information Technology & People 32.5, pp. 1184-215.

Murdoch, B. (2021), "Privacy and Artificial Intelligence: Challenges for Protecting Health Information in a New Era," 2021 BMC Medical Ethics 22.1, pp. 1-6.

Reynolds, D. (2023). Everyone is victimized or only the naïve? The conflicting discourses surrounding identity theft victimization. International Review of Victimology, 29(3), 449-465.

Reyns, B. W. (2013). Online Routines and Identity Theft Victimization: Further Expanding Routine Activity Theory beyond Direct-Contact Offenses. Journal of Research in Crime and Delinquency, 50(2), 216–238

Ryan Randa & Bradford W. Reyns (2019): The Physical and Emotional Toll of Identity Theft Victimization: A Situational and Demographic Analysis of the National Crime Victimization Survey, Deviant Behavior.

Schlackl, F., Link, N., Hoehle, H. (2022), "Antecedents and Consequences of Data Breaches: A Systematic Review," 2022 Information & Management 59.4 103638.

Stojakovic N, D'Alessio SJ, Stolzenberg L. Intangible Identity Theft and Intimate Partner Violence. Violence and Victims. 2023 Dec;38(6):819-838.

Sullins, L. (2006), "Phishing for solution: domestic and international approaches to decreasing online identity theft," 2006 Emory International Law Review 20(1), pp. 397-434.

Ylang, N. (2020), "Capable guardianship against identity theft: Demographic insights based on a national sample of US adults", Journal of Financial Crime, Vol. 27 No. 1, pp. 130-142.

Tajpour A., Zamani, M. (2021), Identity Theft and Prevention, in Tanwar R., et al., Information Security and Optimization, Taylor and Francis, New York.

Van der Meulen, N. (2011), Financial Identity Theft. Context, challenges and countermeasures, The Hague, T.M.C. Asser Press, 2011.

Williams, M.L., (2016), "Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level," 2016 The British Journal of Criminology 56(1), pp. 21-48.