UNIVERSITÀ DEGLI STUDI DI PADOVA

Dipartimento di Diritto Privato e Critica del Diritto
Dipartimento di Diritto Pubblico, Internazionale e Comunitario

Corso di Laurea Magistrale in
Giurisprudenza

Anno Accademico 2022/2023

Phishing e diritto penale: profili problematici

Relatore:
Angelo Zambusi

Controrelatore:
Enrico Mario Ambrosetti

Studente:
Veronica Marchiori

A tutti coloro che si sentono diversi
e non riconosciuti

Indice

Introduzione

Nell'era dell'informazione e della connettività digitale, il fenomeno del cybercrime si è rapidamente evoluto, rappresentando una sfida crescente per la società, il diritto e la sicurezza informatica.

L'accesso sempre più diffuso alla tecnologia e la crescente interconnessione delle reti hanno creato un ambiente fertile per l'emergere di nuove forme di criminalità, che sfruttano l'automazione e le tecnologie informatiche per scopi illeciti.

Questo fenomeno ha riscritto le regole del gioco nel mondo della criminalità, portando alla luce il concetto di "cybercrime".

La tesi si propone di esplorare in profondità il complesso mondo del cybercrime, concentrandosi in particolare su una delle sue manifestazioni più insidiose: il phishing.

Il phishing rappresenta un tipo di attacco informatico mirato a ingannare le vittime al fine di ottenere informazioni sensibili, quali dati bancari, password o informazioni personali.

È una minaccia che si nasconde dietro schermi e tastiere, ma che ha conseguenze reali e devastanti per individui e organizzazioni.

Nel corso dei capitoli, sarà analizzato il fenomeno del cybercrime, esaminando la sua evoluzione da semplici reati informatici a una forma sofisticata di criminalità organizzata.

Saranno esplorate anche le varie tecniche di tipizzazione dei reati informatici, fondamentali per comprendere e contrastare questa minaccia in costante mutamento.

Il cuore di questo lavoro si concentrerà sul phishing, un attacco informatico che ha visto una crescente complessità nelle sue fasi di esecuzione e una vasta gamma di varianti, ognuna con un obiettivo comune: l'inganno. Attraverso l'analisi delle fasi del phishing attack e delle diverse tipologie di phishing, si cercherà di gettare luce sulle strategie utilizzate dagli attaccanti digitali.

Con l'evoluzione delle tecnologie, si sono evolute anche le tecniche di *phishing attack*.

Difatti, rappresenta un'evoluzione alquanto pericolosa del *phishing* il *pharming* (composto dalle parole *phishing* e *farming*): esso rappresenta una tecnica di attacco multiplo di utenti, finalizzata ad accedere a dati ed informazioni personali e riservati, senza la necessità per l'utente di aprire alcuna *e-mail*.

In buona sostanza, si tratta di una specie di truffa *on-line* consistente nella manipolazione degli indirizzi *Domain Name Server* (DNS) utilizzati dall'utente, in modo tale che le pagine *web* utilizzate dall'utente, create appositamente dagli *hacker*, non siano quelle originali, sebbene il loro aspetto e la loro grafica siano identici.

Ma non solo, nel corso dell'elaborato verranno passati in rassegna i più noti attacchi, come vengono perpetrati a danno degli utenti e quale tecnologia viene utilizzata.

Ad esempio, una nuova frontiera del *phishing* è lo *"Smshishing",* ovvero il *phishing* attuato via SMS o di applicazioni c.d. "malevole" sugli *smartphone*, mediante i quali gli attaccanti si impossessano dei dati e delle informazioni degli utenti.

A questi viene inviato un messaggio sul proprio telefono portatile, soprattutto da

una fonte affidabile, con l'invito a fare *click* su un *link* e la promessa di un premio o comunque una proposta particolarmente vantaggiosa e, una volta cliccato, si apre un sito creato appositamente, nel quale l'utente dovrà inserire le proprie credenziali che verranno incamerate anche dal *phisher.*

Tale tecnica si è diffusa in occasione del dilagare dei servizi automatizzati che consentono l'invio di una moltitudine di messaggi SMS in una sola volta. Difatti, gli attaccanti inviano messaggi, facendo figurare che il mittente sia un soggetto affidabile, come la banca di cui la vittima è correntista, che di solito seguono uno stesso modello, vale a dire avvisano le vittime in merito alla sussistenza di un urgente bisogno da soddisfare o della necessità di mettersi subito in contatto con il soggetto di riferimento. Qualora la vittima chiami il numero indicato nel messaggio, una voce registrata chiederà i dettagli della carta di credito e del relativo codice PIN, oltre ad altri dati e informazioni di carattere sensibile: pertanto, il *phisher* ha ottenuto ciò per cui ha posto in essere l'attacco.

Con il passare del tempo, la tecnica del *Smshinshing* si è evoluta e sempre più spesso il contenuto degli SMS fraudolenti ricevuti dagli utenti non hanno più ad oggetto la richiesta di effettuare una chiamata verso un numero di telefono specifico*,* bensì di aggiornare i propri *account,* promettendo in cambio delle ricariche premio, oppure di visionare dei siti *web* commerciali e di istituti di credito, chiedendo pertanto l'inserimento delle credenziali tramite *internet.*

Ma di tutto questo se ne parlerà più nel dettaglio infra.

Per rendere concreti i concetti teorici, saranno analizzati alcuni casi pratici, con particolare attenzione a una controversa vicenda legale che coinvolge Poste Italiane e Banca Intesa.

Questo caso ci offrirà l'opportunità di comprendere meglio come il diritto penale si sia adattato alle sfide poste dal cybercrime, anche alla luce della ratifica della Convenzione Cybercrime.

Infine, ci si soffermerà sull'importanza dell'educazione digitale come strumento fondamentale per promuovere una maggiore consapevolezza digitale tra i cittadini di tutte le età. Saranno valorizzate e trattate le sfide specifiche che coinvolgono i minori e gli anziani, gruppi vulnerabili all'interno del panorama digitale, e saranno discusse le misure necessarie per proteggerli dalle truffe online.

In questo contesto, la tesi cerca di offrire una panoramica completa sul fenomeno del phishing, con l'obiettivo di sensibilizzare sulla necessità di proteggere sé stessi e la propria comunità digitale da questa minaccia sempre presente.

Entrando più nel dettaglio, il lavoro si articolerà in quattro capitoli.

Nel primo capitolo verrà effettuata un'introduzione al fenomeno del cybercrime. In particolare, dopo aver operato degli opportuni cenni alla rivoluzione informatica e al suo impatto sui rapporti sociali e giuridici, la trattazione si soffermerà sul passaggio dai computer crime ai cybercrime, per poi procedere ad esaminare questi ultimi e soprattutto le tecniche di tipizzazione dei reati informatici.

Nel secondo capitolo, si entrerà nel “cuore” della trattazione, procedendo ad esaminare più da vicino il fenomeno del phishing, ovvero di quella particolare pratica truffaldina consistente nell'invio di un messaggio di posta elettronica apparentemente proveniente da un istituto di credito o da una società di commercio elettronico reale, con il quale si invita il destinatario a fornire dati riservati (numero di carta di credito, credenziali per accedere al servizio di home

banking), motivando la richiesta con ragioni di ordine tecnico.

In particolare, si procederà ad analizzare le varie fasi e tipologie del phishing attack, con specifico riguardo alle tecniche evolute di attacco.

Il terzo capitolo sarà dedicato all'individuazione della normativa applicabile al phishing, stante l'assenza nel nostro ordinamento di una norma specificamente deputata alla repressione penale di tale fenomeno ormai sempre più diffuso. In tal senso, verrà esaminata la configurabilità di fattispecie penali quali la truffa, il furto di identità, l'accesso abusivo a sistema informatico ed altre frodi informatiche.

Verrà anche analizzato e commentato un caso pratico sottoposto al vaglio del GIP di Milano, ovvero il caso “Poste Italiane e Banca Intesa”, ripercorrendo gli approdi cui è giunto il giudice di merito.

Da ultimo, nel quarto capitolo, incentrato sulle attività di formazione e prevenzione, verranno passate in rassegna le varie campagne poste in essere dalla Polizia di Stato per evitare di essere vittima di phishing.

Ed infatti, al fine di meglio godere del progresso tecnologico, è necessario disporre di idonee competenze.

Educare significa informare e formare, giacché la frequentazione di ambienti digitali senza il possesso di adeguate competenze può determinare situazioni di disagio e anche di pericolo e il rischio più comune è proprio quello del phishing.

L’obiettivo, oggi, è quello di acquisire una cittadinanza digitale.

Il cittadino digitale deve avere specifiche competenze per agire efficacemente a tutela della propria e altrui sicurezza, soprattutto perché il mondo digitale influenza anche la vita quotidiana off line.

Le competenze della sicurezza digitale hanno anche conseguenze rilevanti dal punto di vista economico. Il livello di sicurezza digitale influenza la partecipazione dei consumatori e lo sviluppo dei servizi e dei mercati digitali.

Prima di intraprendere un'educazione digitale, sarebbe utile fare test di autovalutazione al fine di comprendere il livello di formazione digitale posseduto.

CAPITOLO I

Profili generali e nuovi rischi legati all'evoluzione del fenomeno cybercrime

1.1 La rivoluzione informatica e il suo impatto sui rapporti sociali e giuridici

Al giorno d'oggi ci si trova davanti ad una rilevante rivoluzione e trasformazione dell'attività umana, soprattutto comunicativa (basti pensare ai *socialnetwork*[1]), e tutto grazie all'avvento dei nuovi mezzi tecnologici, come la nascita di *Internet*[2], lo sviluppo dei *computer*[3] e degli *smartphone*[4], nonché di ogni altra funzionalità ad essi collegata.

Tutto ciò ha indubbiamente facilitato la nostra quotidianità, agevolando lo svolgimento di una serie di attività effettuate in ambito sociale, lavorativo, politico

[1] I *socialnetwork* sono siti internet che forniscono agli utenti di internet un punto di incontro virtuale per scambiarsi messaggi, chattare, condividere foto e video.

[2] Definizione di *internet* presa dal dizionario di Oxford Languages di google: Rete di collegamenti informatici a livello planetario che permette la connessione e la comunicazione tra loro di reti locali di computer e banche dati, rendendone disponibili agli utenti le informazioni nella forma di immagini, filmati, ipertesti, musica

[3] Definizione di *computer* presa dal dizionario di Oxford Languages di google: apparecchio elettronico in grado di svolgere operazioni matematiche e logiche e di memorizzare informazioni a una velocità e in una quantità superiori a quelle di cui è comunemente capace il cervello umano; nelle sue componenti materiali (*hardware*) è costituito da meccanismi di entrata (*input*) e di uscita (*output*) delle informazioni e da un insieme di circuiti e di dispositivi sui quali si svolgono le funzioni di memoria, di elaborazione e di controllo, che avvengono grazie a programmi contenenti istruzioni (*software*); tali programmi sono basati su un sistema di computazione binario e sono scritti in vari linguaggi di programmazione; oltre ai linguaggi macchina sono stati elaborati anche linguaggi simbolici meno complessi.

[4] Letteralmente significa "telefono intelligente", è un telefono che unisce le funzioni di un telefono semplice a quelle di un computer.

e culturale[5].

Difatti, è evidente come in questo periodo storico si è connessi ad ogni ora del giorno e della notte, si comunica in tempo reale da una parte all'altra del mondo, non esistono più distanze; i nuovi mezzi tecnologici sono diventati, dunque, una sorta di "scatola nera" della nostra più intima personalità[6].

Tuttavia, anche dietro al progresso tecnologico possono nascondersi delle insidie sempre più preoccupanti.

Invero, l'ingresso nella nostra società del digitale e del fenomeno *Internet* hanno rappresentato un terreno sempre più fertile per la diffusione di nuove condotte ed attività illecite connesse a "*modalità, oggetti o attività di carattere tecnologico ovvero a fattispecie incriminatrici comuni che possono vedersi configurare anche attraverso la rete o nel cyberspace"*[7].

L'aumento della diffusione delle fattispecie criminose legate al mondo informatico ha contribuito alla trasformazione della fisionomia delle "tradizionali" forme di criminalità, al punto tale da spingere la dottrina contemporanea a fare utilizzo di

---

[5] STAZI A., *Commercio elettronico ed utilità delle informazioni da fornire ai clienti*, in *Dir. dell'inf.*, 2009, p. 5 s.

[6] SERICOLA E., *Cybercrime e diritti fondamentali nell'era di Internet,* in *Filodiritto*, 9 maggio 2017, p. 1. L'autore vuole dirci che grazie ad internet non ci sono più ostacoli di natura spazio-temporale e che, grazie ai telefoni, siamo sempre connessi e che gli smartphone sono in grado di registrare le nostre preferenze, le nostre ricerche e, grazie agli algoritmi suggerirci, per esempio, pubblicità.

[7] Il termine *cyberspace* fece la sua prima comparsa nel 1982 in un racconto di fantascienza intitolato *Burning Chrome* (tradotto: *La notte che bruciammo Chrome,* 1989), pubblicato da William Gibson sulla rivista Omni. Sebbene lo spazio individuato da Gibson fosse inizialmente connesso a fenomeni di fantascienza e di illusioni tecnologiche, nel terzo millennio esso inizia ad essere utilizzato quale sinonimo di Internet, mediante un uso frequente di metafore spaziali: sullo spazio Internet si può navigare, esplorare, acquistare domini, ecc.

termini quali *cyber crime* o *computer crime*[8] al fine di indicare le condotte violative di interessi penalmente rilevanti riconducibili alla “criminalità informatica” la quale, a sua volta, può ricomprendere sia i c.d. reati informatici in senso stretto che quelli in senso lato, a seconda che gli stessi reati siano pertinenti a modalità, oggetti o attività aventi carattere digitale, oppure siano realizzati per mezzo della stessa tecnologia, della rete o nel *cyberspace*[9].

Difatti, le manifestazioni criminose che vengono poste in essere sul *web* hanno assunto nuove e diverse configurazioni, le quali trovano crescente rilievo offensivo ed allarmante impatto sociale e che necessitano di una risposta normativa.

Con l'entrata in vigore del Trattato di Lisbona, l'art. 83 TFUE ha inserito la “criminalità informatica” tra i fenomeni criminosi di natura grave e transnazionale su cui l'Unione Europea ha competenza penale.

In ambito europeo sono già state approntate diverse iniziative in materia, di cui si procede a ricordarne alcune:

- la direttiva relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, che sostituisce la decisione quadro

[8] Letteralmente significa reato del cyberspazio e reato da computer, reato cibernetico o reato informatico. Nel merito sono i reati commessi grazie all’uso di internet o del computer, o reati commessi nel cyberspazio.

[9] FLOR R., *Lotta alla criminalità informatica e tutela di tradizionali e nuovi diritti fondamentali nell'era di Internet,* in *Diritto Penale Contemporaneo,* 20 settembre 2012. L’autore riprende le note definizioni di cyber crime e computer crime ossia i reati cibernetici e i reati informatici distinguendo quelli commessi su internet e quelli commessi grazie all’uso di computer, come meglio si dirà infra.

2004/68/GAI del Consiglio, del 13 dicembre 2011[10];

- la proposta di direttiva del Parlamento europeo del Consiglio COM (2010) 517 – C7 - 0293/2010 – 2010/0273(COD), riguardante gli attacchi contro i sistemi informatici, che sostituisce la decisione quadro 2005/222/GAI[11];

- già anteriormente all'entrata in vigore del Trattato di Lisbona, le proposte di direttiva e di decisione quadro riguardanti le misure penali predisposte per assicurare il rispetto dei diritti di proprietà intellettuale[12];

- nel settore della tutela dei diritti di autore, ulteriormente alle numerose iniziative non riguardanti propriamente la materia penale, ma che hanno spinto la maggior parte degli Stati all'adozione di strumenti di tutela penale – a partire dal Libro verde "*Il diritto di autore e le sfide tecnologiche – Problemi di diritto di autore che richiedono un'azione immediata"* del 1988 – nonché alle direttive predisposte a tutela dei *software*, delle banche dati e di attuazione agli obblighi internazionali che derivano dai trattati;

- la comunicazione della Commissione al Consiglio e al Parlamento europeo del 28 marzo 2012, sulla "*Lotta alla criminalità nell'era digitale:*

[10] VERRI A., *Contenuto ed effetti (attuali e futuri) della direttiva 2011/93/UE,* in *Dir. Pen. Cont.,* 28 marzo 2012. L'autore analizza la direttiva relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, che sostituisce la decisione quadro 2004/68/GAI del Consiglio, del 13 dicembre 2011.

[11]Proposta di direttiva del Parlamento europeo e del Consiglio COM (2010)517 - C7-0293/2010 - 2010/0273(COD), relativa agli attacchi contro i sistemi di informazione, che abroga la decisione quadro 2005/222/GAI.

[12] FLOR R., *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di Internet,* Padova, 2010, p. 48.

istituzione di un centro europeo per la lotta alla criminalità informatica"[13]*,* nella quale si legge che la lotta alla criminalità informatica, il cui strumento giuridico principale è la Convenzione del Consiglio di Europa sulla criminalità informatica, continua ad essere una priorità principale. Pertanto, è parte integrante del ciclo programmatico dell'UE al fine di contrastare la criminalità organizzata e le forme gravi di criminalità internazionale e rientra tra gli sforzi finalizzati allo sviluppo di una strategia generale dell'UE per rafforzare la sicurezza informatica[14].

Tali iniziative si caratterizzano per due elementi comuni, ovvero l'alta potenzialità criminogena delle nuove tecnologie della comunicazione e dell'informazione, nonché la necessità di un intervento europeo e di politica criminale europea al fine di contrastare i reati commessi su *Internet* o attraverso la rete[15].

1.1.1 Il fattore umano nel cybercrime: tecniche di persuasione e induzione all'azione richiesta dall'hacker

Il tema del fattore umano nel cybercrime e le tecniche di persuasione e induzione all'azione utilizzate dagli hacker è di grande importanza. Questo aspetto è cruciale da comprendere poiché gran parte delle violazioni di sicurezza informatica coinvolgono l'interazione umana, spesso sfruttata in modi subdoli

[13] COM (2012) 140 final.

[14] VALSECCHI A., *Brevi osservazioni di diritto penale sostanziale*, in *Diritto penale processuale*, 2005, p. 44 ss.

[15] STAZI A., *Commercio elettronico ed utilità delle informazioni da fornire ai clienti*, in *Dir. dell'inf.*, 2009, p. 19 ss.

dagli attaccanti.

Un metodo ampiamente diffuso è il "phishing", dove gli hacker inviano e-mail o messaggi apparentemente legittimi per ingannare le vittime. Questi messaggi possono sembrar provenire da banche, servizi online o aziende con cui si ha a che fare regolarmente. L'intento è persuadere le vittime a rivelare informazioni sensibili come password o dati finanziari, spesso chiedendo di cliccare su link o scaricare file dannosi[16].

L'ingegneria sociale è un'altra tattica potente, che impiega la manipolazione psicologica. Gli hacker si fingono amici, colleghi o persino membri della famiglia per ottenere informazioni confidenziali o spingere le vittime a compiere azioni che potrebbero causare danni.

Un altro approccio è l'uso di pretesti credibili, come finger di essere tecnici IT in missione di manutenzione urgente. Questi pretesti cercano di convincere la vittima a fornire accesso al proprio sistema.

L'autorità fittizia è una tecnica in cui gli hacker si spacciano per figure di autorità, minacciando azioni legali o conseguenze gravi per indurre la vittima a seguire le loro richieste[17].

La scarsità è un altro strumento psicologico, in cui gli hacker fanno credere alla vittima che ci sia urgenza o pericolo imminente. Questo può mettere la vittima sotto pressione per agire senza pensarci troppo.

La convinzione reciproca è un approccio subdolo in cui gli hacker cercano di

---

[16] ZICCARDI G., *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Milano, 2015, p. 19 s.

[17] ZANASI A., *Nuove forme di guerra, nuove forme di intelligence: Text Mining. Intelligence in XXI Century*, Roma, 2001, p. 99 s.

creare un senso di complicità o solidarietà tra loro e la vittima, spingendola a compiere azioni che potrebbero sembrare "necessarie" per risolvere un problema immaginario. Le tecniche di pressione emotiva sfruttano emozioni come la paura, la curiosità o la compassione per ottenere la collaborazione della vittima[18].

Infine, i falsi premi o incentivi vengono promessi dagli hacker per attirare le vittime. Questi possono includere promesse di ricompense o sconti allettanti.

Per difendersi da queste minacce, è essenziale essere consapevoli dei rischi e adottare misure di sicurezza solide, come l'utilizzo di software antivirus, la verifica delle fonti delle comunicazioni online e la protezione delle informazioni sensibili. Inoltre, l'educazione sulla sicurezza informatica e la promozione di una cultura di sicurezza sono fondamentali per ridurre il rischio di cadere vittima di queste tecniche di manipolazione[19].

1.2 La rilevanza giuridico-penale dell'"automazione"

Come innanzi accennato, la rivoluzione "cibernetica" ha avuto un forte impatto sui rapporti sociali e giuridici, determinando anche dei rilevanti mutamenti per il diritto penale.

In tal senso, il primo aspetto innovativo è rappresentato dall'automazione, la quale di volta in volta ha preso il posto di importanti attività umane, come riconosciuto anche nelle definizioni giuridiche di "dati" e "sistemi informatici"

[18] ZICCARDI G., *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Milano, 2015, p. 32 s.

[19] ZANASI A., *Nuove forme di guerra, nuove forme di intelligence: Text Mining. Intelligence in XXI Century*, Roma, 2001, p. 89 ss.

contenute nelle fonti sovranazionali.

Alla fine del secolo scorso, il "*boom*[20]*"* registrato da Internet ha trasformato globalmente il modo di comunicare, anche grazie alla diffusione dei dispositivi mobili e all'estensione delle coperture di connessione, rappresentando attualmente uno "spazio" (appunto, il *cyberspace*) di costante scambio e comunicazione.

Ed infatti, nel *cyberspace* si dislocano, sempre più, delle attività individuali e collettivi di vario tipo, che vanno dal tempo libero, al commercio, dall'economia alla cultura, fino alla politica. In esso, gli utenti possono ricoprire al contempo il ruolo di autori o vittime di reati e condotte criminose, a causa della crescente estensione ed importanza che i dati e i contenuti hanno assunto sul *web,* i quali vengono memorizzati, elaborati e gestiti su piattaforme informatiche e reti sociali da sistemi esperti e motori di ricerca sempre più potenti, determinando una progressiva concentrazione di poteri in capo agli *Internet Service Provider* (ISP) che ne siano titolari e li controllino[21].

L'effetto che tale rivoluzione informatica ha avuto sul diritto penale è rappresentato – come si dirà anche più diffusamente nel prosieguo della trattazione – dal passaggio dal concetto di "*computer crime*" (ovvero reato informatico) a quello di *cybercrime* (reato cibernetico).

---

[20] "Boom" è inglese e viene italianizzato in "bum" quando è un'onomatopea. Quando invece si parla di "boom economico" o "boom di dati" si usa di solito l'inglese. Rappresenta il suono onomatopeico di un'esplosione tipico dei fumetti in inglese.

[21] B.N. Romano, Il rischio di "attacchi" ai sistemi informatici tra fattispecie penalmente rilevanti, tutela dei dati ed esigenze di "buona amministrazione", in *Amministrativ@mente* 3, 2021, pp. 545-594.

Oggi come oggi, possono essere commessi per il tramite o ai danni di sistemi e strumenti informatici nel *cyberspace*, oltre ai reati informatici in senso stretto[22], anche reati di ogni altro tipo, i cui elementi costitutivi o circostanziali, in via alternativa o interpretativa, consentono in ogni caso di sussumerli nelle specifiche fattispecie incriminatrici.

In tal senso, può dunque parlarsi di "reati informatici in senso ampio "o di "reati cibernetici", i quali ricomprendono tutti quelli la cui commissione viene realizzata o possa realizzarsi nel *web*, potendo essa rappresentare sia un elemento espresso che un elemento compatibile soltanto in via interpretativa con la fattispecie legale (si pensi alla diffamazione *on-line*, alla diffusione di materiale pedopornografico, all'istigazione alla discriminazione e all'odio razziale, ma anche ad estorsioni, riciclaggio, reati di violazione della *privacy*[23] e dei diritti di autore)[24].

Anche la sistemazione di tali diverse categorie di reati informatici e cibernetici – ormai ampiamente presenti nel codice penale o nella legislazione speciale (in specie in materia di protezione dei dati personali e di diritti di autore), evidenzia la grande varietà ed importanza dei beni giuridici protetti, i quali possono

[22] I reati informatici in senso stretto si caratterizzano per la previsione, nella fattispecie legale, di specifici elementi di tipizzazione, contenenti un esplicito riferimento alle nuove tecnologie dell'informazione o della comunicazione (c.d TIC), siano essi relativi alla condotta o ai mezzi, alle modalità, agli effetti o ad ogni altro elemento essenziale o circostanziale: si pensi all'accesso abusivo ad un sistema informatico, la frode informatica, il falso in documenti informatici.

[23] In italiano: riservatezza

[24] C. Crescioli, *Le diverse fasi dei "phishing attacks": le fattispecie vigenti e i problemi applicativi in prospettiva comparata tra Italia e Germania*, in *L'Indice penale*, 3, 2021, pp. 799-831.

presentare, nella nuova dimensione cibernetica, dei propri profili di novità, come emerge chiaramente nei reati contro la riservatezza informatica e la sicurezza informatica[25].

1.3 Il passaggio dai *computer crime* ai *cybercrime*

Dal punto di vista giuridico, non si rinviene una categoria definita di "criminalità informatica", sebbene tale terminologia compaia nelle fonti europee e sovranazionali[26].

Parimenti è a dirsi con riguardo ai concetti di "*computer crime"*, "*computer related crime*" o "*cybercrime*", dei quali non si rinviene una definizione riconosciuta a livello internazionale.

Dal punto di vista empirico, la criminalità informatica ricomprende in sé una vasta gamma di comportamenti che si pongono in violazione di interessi rilevanti penalmente – riconducibili a "reati informatici" - introdotti in diversi ordinamenti nazionali.

Sotto il profilo fenomenico, a seguito della vasta diffusione di Internet, si è assistiti al passaggio dalla dimensione "privata" o "individuale" del *computer* e delle reti di computer, alla dimensione "pubblica" o "collettiva" dei sistemi, fondati

[25] ZANASI A., *Nuove forme di guerra, nuove forme di intelligence: Text Mining. Intelligence in XXI Century*, Roma, 2001, p. 55 ss.

[26] BRIAT M., SIEBER U., *Computer Related Criminality Analysis of Legal Policy in the OECD Area,* Parigi, 1986. Secondo gli autori la criminalità informatica non consiste in una categoria definita giuridicamente.

sull'interconnettività globale.

Pertanto, nella moderna società dell'informazione, emerge il carattere flessibile ed aperto del fenomeno della criminalità informatica nei confronti di fatti criminosi che possono essere commessi mediante la rete o nel *cyberspace.*

Dal punto di vista del diritto penale sostanziale, la criminalità informatica può ricomprendere sia fattispecie legali formulate con elementi di tipizzazione collegati a processi di automatizzazione dei dati o informazioni, ovvero legate a modalità, oggetti o attività di carattere tecnologico (reati informatici in senso stretto)[27], sia quelle fattispecie delittuose "comuni" le quali, sebbene non presentino in via espressa degli elementi tipici caratterizzati dalla tecnologia, possono essere applicate a fatti commessi per il tramite della tecnologia, la rete o nel *cyberspace*[28].

In tal contesto, diviene particolarmente rilevante anche la distinzione tra reati cibernetici in senso stretto e reati cibernetici in senso lato.

Nel primo caso, l'elemento specializzante è rappresentato proprio dalla connessione in rete o dalla fruibilità del *cyberspace*[29]*.*

---

[27] PICOTTI L., *Biens juridiques protégés et techniques de formulation des incriminations en droit pénal de l'informatique,* in *Rev. Int. Droit pénal*, 2006, n. 3/4, p. 525. L'autore fa riferimento al reato di truffa comune (art. 640 c.p.), che può essere commessa attraverso l'invio di e-mail ingannevoli che inducono in errore il destinatario determinandolo ad effettuare un atto di disposizione patrimoniale su conti correnti online. Sempre l'autore, inoltre, fa riferimento alla diffamazione online, o alle forme di manifestazione o diffusione del pensiero o di contenuti illeciti, quale la rivelazione od agevolazione "in qualsiasi modo" della conoscenza, da parte di terzi non legittimati, di una notizia che debba rimanere segreta.

[28] *Ibidem.*

[29] Ai meri fini esemplificativi, si considerino gli artt. 171, lett. a) *bis* e 171 *ter*, co. 2, lett. a) *bis* della l. n. 633/41 (che sanzionano la diffusione abusiva tramite l'immissione in un sistema di reti telematiche di un'opera dell'ingegno protetta).

I secondi, invece, sono formulati in termini maggiormente generali, tanto da poter essere realizzati o concepiti a prescindere dall'informatica e dalla rete[30].

Tale impostazione teorica rinviene un riscontro nelle disposizioni di stampo processuale previste dalla Convenzione sulla criminalità informatica del Consiglio d'Europa, le quali trovano applicazione non soltanto ai reati previsti dalla stessa (artt. 2-11), bensì a tutte le fattispecie incriminatrici commesse per il tramite dei sistemi informatici e agli illeciti per il cui accertamento si richiede la raccolta della prova elettronica (*ex* art. 14 Convenzione).

Parte della dottrina americana sostiene che la categoria dei *cybercrime* comprende in sé almeno tre *sub*-categorie:

- reati in cui il *computer* o il sistema informatico rappresentano il fine delle attività criminali;
- reati in cui il computer e, in generale, le nuove tecnologie ed il *web* rappresentano degli strumenti per commettere o preparare un reato;
- reati in cui il sistema informatico e la rete costituiscono solo un "aspetto incidentale" nella commissione dell'illecito[31].

---

[30] PICOTTI L., *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee,* in *Riv. Trim. dir. Pen. ec.,* 2011, p. 827. Secondo l'autore nell'ordinamento italiano, reati come l'accesso abusivo a sistemi informatici (art. 615 ter c.p.) o la frode informatica (art. 640 ter c.p.) sono reati informatici che si connotano per un nuovo oggetto passivo su cui la condotta va a cadere (quali i dati, le informazioni, i programmi od altri "prodotti" informatici o digitali, compresi i "sistemi informatici" in genere) oppure si caratterizzano per il fatto che il computer ed i prodotti informatici in genere costituiscono lo strumento tipico di realizzazione del 'fatto' criminoso.

[31] BRENNER S., *Defining Cybercrime: a review of Federal and State Law,* in CLIFFORD R.D., *Cybercrime,* p. 104. L'Autrice si chiede se la categoria "cybercrime" abbracci nuove forme di criminalità e di crimini, ovvero se non si tratti piuttosto di reati vecchi rivisti in una nuova ottica.

1.4 Le tecniche di tipizzazione dei reati informatici

La nuova categoria della criminalità cibernetica non può più essere circoscritta ad un numero limitato di reati e, pertanto, di vittime potenziali, bensì include attualmente un numero potenzialmente indefinito di illeciti e di modalità offensive dei diritti e degli interessi altrui, alcuni dei quali sono anche di nuova creazione, quale esito dello stesso sviluppo tecnologico[32].

In tal senso, può essere ricompresi tra i crimini cibernetici – se realizzato nel cyberspazio – l'estorsione posta in essere mediante la criptazione illecita dei dati di un sistema informatico altrui, per il tramite dell'installazione abusiva da remoto di un *malware*[33], il quale realizzi in tal modo una forma di violenza informatica, come definita dall'art. 392, comma 3, c.p.[34], ove la vittima viene costretta, al fine di riacquistare la libera disponibilità dei propri dati, a corrispondere un ingiusto prezzo di riscatto per ottenere l'indispensabile chiave di decriptazione, con conseguente consumazione del delitto di cui all'art. 629 c.p.[35].

---

[32] E. Stringhi, *La minaccia del "deepfake" ed i rischi per la "cybersecurity" delle organizzazioni economiche: un approccio pratico*, in *Ciberspazio e Diritto*, 1, 2021, pp. 59-77.

[33] Programma, documento o messaggio di posta elettronica in grado di apportare danni a un sistema informatico.

[34] L'art. 392, comma 3, c.p. - rubricato "*Esercizio arbitrario delle proprie ragioni con violenza sulle cose"* - prevede espressamente che: "*si ha altresì violenza sulle cose allorché un programma informatico viene alterato, modificato o cancellato in tutto o in parte ovvero impedito o turbato il funzionamento di un sistema informatico o telematico"*.

[35] Il reato di estorsione di cui all'art. 629 c.p afferma espressamente che: "*chiunque, mediante violenza o minaccia, costringendo taluno a fare o ad omettere qualche cosa, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da cinque a dieci anni e con la multa da euro 1.000 ad euro 4.000.*

La pena è della reclusione da sette a venti anni e della multa da euro 5.000 ad euro

Da tanto emerge la varietà delle modalità di condotta e delle tecniche di commissione dei reati cibernetici, oltrepassando il novero di quelli consistenti nella “comunicazione” o “diffusione” di un pensiero o di contenuti illeciti sul *web*, sebbene essi mantengano un ruolo particolarmente rilevante.

Da ciò deriva anche una corrispondente diversificazione dei beni giuridici penalmente rilevanti e delle vittime meritevoli di tutela che ne sono titolari, le quali sono spesso ignare, sia che si tratti di individui o categorie collettive, a partire dai minori sino a quelle soggette a discriminazioni[36].

Indicativa in tal senso è proprio la necessità di tutelare penalmente la riservatezza nel *cyberspace,* la quale, da una parte, si eleva alla nuova dimensione della riservatezza informatica, quale autonomo bene giuridico nonché diritto fondamentale della persona, da intendere quale diritto ad uno spazio informatico esclusivo, il quale va lasciato libero da intrusioni da parte di soggetti terzi.

In tal senso, esso assurge a strumento essenziale al fine di realizzare pienamente l'individuo nell'attuale vita sociale, il quale non può essere compromesso nemmeno dalla pubblica autorità, se non nei casi e nei modi previsti in via tassativa dalla legge, unitamente alle garanzie del controllo giudiziario[37].

Dall'altra parte, si può affermare che la riservatezza è altra cosa rispetto alla

---

15.000, se concorre taluna delle circostanze indicate nell'ultimo capoverso dell'articolo precedente”.

[36] B. Russo, *I nuovi orientamenti giurisprudenziali sul reato di "phishing": “La banca è responsabile se non prova che il cliente ha disposto il pagamento”*, in *Rivista di diritto bancario*, 4, 2019, 2, pp. 71-87.

[37] FLOR R., *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d online-Durchsuchung*, in *Riv. trim. dir. pen. ec*., 2009, p. 69.

privacy in senso stretto, la quale indica più propriamente il diritto alla tutela dei propri dati personali, che ha assunto caratteristiche particolari, richiedendo attualmente nuove forme di tutela, finalizzate a garantire la possibilità di controllo da parte della persona cui si riferiscono le informazioni e il bilanciamento con la contrapposta esigenza di circolazione e di accessibilità anche da parte di terzi, in quanto elementi spesso essenziali per numerose attività e servizi in ogni settore della vita moderna.

L'importanza di tale bene giuridico rende necessario un intervento pubblico efficace di tutela il quale, in mancanza di sufficiente capacità preventiva di sanzioni soltanto civilistiche e amministrative – da valutare anche dal punto di vista degli strumenti di ricerca e di raccolta delle prove – deve includere anche misure penali[38].

Parimenti rilevante è anche il nuovo bene giuridico della "*cybersecurity*" o sicurezza informatica, il quale non è soltanto posto a protezione degli altri interessi e diritti della persona meritevoli di tutela nel *cyberspace* – a partire dalla riservatezza informatica e dalla *privacy* sopra menzionate – bensì è a sua volta meritevole di autonoma protezione giuridica, ivi compresa quella penale, poiché svolge una funzione di garanzia "preventiva" di tutti gli altri interessi e diritti che emergono e si esercitano nello spazio cibernetico, al punto da divenire, a determinate condizioni, indisponibile per gli altri titolari dei sistemi informatici, in quanto collettivamente condiviso, nella dimensione globale e di stretta

[38] PICOTTI L., *Sicurezza informatica e diritto penale,* in DONINI, PAVARINI, *Sicurezza e diritto penale,* Bologna, 2011, p. 66 ss.

interdipendenza che hanno i rapporti e le attività sul *web*[39].

Proprio tale interdipendenza, assunta dalla sicurezza e dalla riservatezza, parimenti agli altri beni e diritti nel *cyberspace*, sta a dimostrare il crescente ruolo rivestito dagli *Internet Service Providers* (ISP), i quali, in relazione ai diversi servizi e alle numerose attività che vi si svolgono, diventano anche centri di imputazione di responsabilità – civili, penali ed amministrative – il cui fondamento positivo e la cui delimitazione pongono dei problemi giuridici, non risolti dalla vecchia regolamentazione, risalente all'originario modello delineato dal *Millennium Copyright Act* americano del 1997 nonché dalla Direttiva CE 2000/31 relativa al commercio elettronico, che lo ha in parte ricalcato e sulla cui inadeguatezza occorrerà effettuare degli ulteriori cenni[40].

1.5 Il *cybercrime* quale nuovo volto della criminalità organizzata

La criminalità si pone alla continua ricerca di luoghi privi di controllo per realizzare in tranquillità i propri affari criminosi. In tal senso, il *web* rappresenta senza dubbio una “zona franca”, poiché in grado di fornire delle sufficienti garanzie di sicurezza e di anonimato[41].

---

[39] PICOTTI, *Sicurezza informatica e diritto penale,* in DONINI, PAVARINI, *Sicurezza e diritto penale,* Bologna, 2011, p. 217.

[40] PICOTTI L., *Sicurezza informatica e diritto penale,* in DONINI, PAVARINI, *Sicurezza e diritto penale,* Bologna, 2011, p. 89 s.

[41] ROMANO B.N., *Il rischio di "attacchi" ai sistemi informatici tra fattispecie penalmente rilevanti, tutela dei dati ed esigenze di "buona amministrazione"*, in Amministrativ@mente, 3, 2021.

Si è assistito dunque alla proliferazione di condotte illecite commesse in rete.

La diffusione degli strumenti informatici ha generato delle trasformazioni sociali molto significative, non sempre positive. Il mondo criminale, infatti, ha intuito ben presto le potenzialità degli strumenti operativi informatici per finalità di tipo illecito. A ciò bisogna aggiungere anche coloro che, stimolati dalla volontà di dimostrare la propria abilità o genialità informatica, quasi per gioco o per sfida, hanno cominciato a commettere piccoli e grandi crimini informatici, con conseguenze negative molto significative[42].

[42] Cfr., sul punto, Destito V., *Reati informatici*, in *Digesto delle discipline pubblicistiche*, XVIII, Milano, 2010, pp. 141 s., il quale osserva che «tali soggetti, nel linguaggio informatico, vengono distinti in hacker e cracker. Il termine hacker nasce con l'informatica ed è rivolto ad identificare chi attacca strumenti informatici con il solo scopo di capirli e smontarli, senza arrecare danno o sottrarre informazioni. Il termine deriva dal verbo inglese "to hack" che tradotto significa "scomporre, fare a pezzi". Lo scopo dell'hacker non è quello di inserirsi in un sistema informatico per danneggiarlo o per appropriarsi di informazioni altrui. Lo scopo che si propone un hacker è quello della sfida, provare ad accedere ad un sistema informativo protetto per capire come funziona, per scomporlo e studiarlo, senza danneggiarlo. I media, nel tempo, hanno mal interpretato il significato di hacker e lo hanno sostituito al meno noto termine "cracker". Quest'ultimo deriva da un altro verbo inglese "to crack" che ha ben altro significato: "distruggere". Da questa precisazione è possibile comprendere la sostanziale differenza che c'è tra un hacker ed un cracker. Le tecniche utilizzate sono sostanzialmente le stesse ma i primi si limitano allo studio del loro obiettivo, mentre gli altri si addentrano nel sistema informatico con lo scopo di danneggiare i dati o di appropriarsene. Spesso questi termini vengono utilizzati come sinonimi uno dell'altro ma la differenza è sostanziale soprattutto per il fatto che la condotta tipica di un hacker è quella di accedere ad un sistema informatico e lasciarvi una traccia del suo passaggio a sola dimostrazione di essere riuscito a compiere l'atto, mentre i crackers agiscono con lo scopo di danneggiare il sistema attaccato, spesso per il solo gusto di farlo. Noti sono i tentativi di danneggiamento

La diffusione dell'informatica, dunque, soprattutto dopo l'apertura al pubblico dell'accesso ed utilizzo di Internet, collocabile a metà degli anni novanta del secolo scorso, «ha determinato la comparsa e lo sviluppo crescente di "nuovi" reati, che si manifestano sia come reati informatici "in senso stretto" (vale a dire che già a livello normativo, a seguito della loro specifica incriminazione da parte del legislatore, richiedono necessariamente fra gli elementi costitutivi l'utilizzo delle tecnologie e dei prodotti informatici, o la produzione di effetti tipici su di essi: si pensi alle frodi informatiche, ai falsi ed ai danneggiamenti informatici, agli accessi abusivi a sistemi informatici ecc.), sia come reati informatici "in senso ampio" ed, in specie, come reati "cibernetici"»[43].

---

compiuti contro le grandi società di software multinazionali, al solo scopo di danneggiarle, ad esempio oscurando i loro server o attaccandole con potenti virus».

[43] Così Picotti L., *I diritti fondamentali nell'uso ed abuso dei social network. Aspetti penali*, in *Giurisprudenza di merito*, 12, 2012, p. 2552. L'A. osserva che «la tumultuosa diffusione dei social network, che costituisce uno dei più recenti ed eclatanti effetti dell'impatto di Internet sulle relazioni interpersonali fra soggetti di ogni età, professione, estrazione sociale, ma in particolar modo fra i giovani — oltre che fra e con enti di qualsiasi natura — dimostra la grande rilevanza non solo dell'evoluzione tecnologica, ma ancor più della sua capillare penetrazione nella società contemporanea, in cui determina rilevanti cambiamenti dei modi della comunicazione e diffusione delle idee e delle informazioni, dei tempi e contenuti del confronto sociale, del costume stesso, condizionando o modellando lo svolgersi di comportamenti collettivi ed individuali anche nel mondo «reale», come dimostrano emblematicamente gli incontri, i dibattiti, le manifestazioni, i movimenti politici che si organizzano in brevissimo tempo in rete ovvero i fatti eclatanti e addirittura i tragici epiloghi posti in essere da singole persone per effetto di quanto accaduto o preannunciato in un social network». Ancora, l'A. ritiene che «i reati informatici, pur essendo concepibili o tipizzati anche a prescindere dal riferimento alla tecnologia informatica e ad Internet, trovano in detti strumenti ed, in generale, nel Cyberspace una peculiare possibilità e modalità di realizzazione, che li rende solitamente più temibili o dannosi: tanto da richiedere una più specifica e spesso più

L'avvento dell'informatica, dunque, chiama il diritto penale ad affrontare una nuova sfida, che risiede soprattutto nella necessità di contrastare questi nuovi fenomeni criminali senza violare i principi fondamentali e garantisti del diritto penale. Va segnalato, a tal proposito, che il codice penale è stato pensato e scritto in un periodo storico in cui l'informatica era del tutto assente, ragion per cui l'interprete è stato costretto, almeno fino ai primi interventi normativi, a ricorrere ad interpretazioni estensive, con tutte le difficoltà e le molteplici insidie legate alla possibile violazione dei principi fondamentali del diritto penale[44].

Infatti, in presenza di esigenze politico criminali, nonché in considerazione del fatto che si tratta indubbiamente di condotte socialmente disprezzabili, in assenza di una normativa ben definita si corre il rischio di sacrificare i principi propri del diritto penale pur di sanzionare le suddette condotte. Ciò ha spinto il legislatore italiano ad intervenire proprio al fine di evitare le suddette aporie. La disciplina normativa in materia di reati informatici è stata introdotta per la prima volta in Italia con la legge n. 23 dicembre 1993, n. 547, recante "Modificazioni ed integrazioni alle norme del Codice penale e del Codice di procedura penale in tema di criminalità informatica"[45].

---

severa risposta penale (si pensi alla pedopornografia ed alle violazioni dei diritti d'autore, ma anche alla diffamazione e ad altri reati di "manifestazione del pensiero" on line: ponendo nel contempo peculiari problemi di natura processuale, in particolare per quanto riguarda le modalità e le condizioni di raccolta, conservazione ed utilizzazione delle c.d. prove elettroniche».

[44] ROMANO B.N., *Il rischio di "attacchi" ai sistemi informatici tra fattispecie penalmente rilevanti, tutela dei dati ed esigenze di "buona amministrazione"*, in Amministrativ@mente, 3, 2021

[45] Ibidem.

La *ratio* della legge risiede anzitutto nell'esigenza di arginare il fenomeno, ormai sempre più diffuso, della criminalità informatica, la cui recrudescenza si deve proprio all'affermarsi di Internet che, nel suo rivoluzionare il mondo in tutti gli aspetti, modo di comunicare compreso, si è rivelato un terreno fertile per la diffusione di un nuovo modo di intendere la criminalità. L'illusione dell'anonimato e l'abbattimento di ogni barriera fisica hanno favorito la criminalità via Internet, imponendo al legislatore di intervenire[46].

La criminalità, dunque, ha compreso le potenzialità sterminate di Internet, e ha con il tempo perfezionato gli strumenti e le tecniche dirette a commettere reati mediante il web. Non è da sottovalutare anche un problema culturale: la percezione, infatti, molto spesso, è che i criminali informatici siano diversi dai criminali di strada, come se le loro azioni fossero connotate da un disvalore minore solo perché non aggrediscono fisicamente la vittima, ma solo in modalità virtuale.

Prima del suddetto intervento normativo, la dottrina e la giurisprudenza avevano fatto ricorso, per sanzionare i crimini informatici, alla cornice normativa preesistente, scontrandosi tuttavia spesso con paletti ed ostacoli del tutto insormontabili. Le fattispecie tradizionali (si pensi, per fare un esempio, alla truffa, con la quale si punivano i reati di frode informatica) si erano rivelate del tutto incapaci di cogliere le peculiarità dei crimini informatici. I reati introdotti dalla legge in esame sono numerosi, e non possono essere analizzati tutti in questa

[46] Cfr., sul tema, Contrafatto V., *Reati informatici*, Vicalvi, Key Editore, 2017, p. 1 ss.

sede[47], in quanto altrimenti ciò ci condurrebbe lontano dai fini dell'indagine.

A seguito dell'intervento normativo attuato con legge n. 147/1993, il legislatore è nuovamente intervenuto con la legge 18 marzo 2008, n. 48, con la quale è stata ratificata, non senza ritardo, la Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica, approvata nella capitale ungherese il lontano 23 novembre 2001.

L'intervento legislativo è molto importante perché ha introdotto significative modifiche alle disposizioni penali processuali e sostanziali, in tema di reati informatici, garantendo, finalmente, l'adeguamento della vetusta cornice normativa italiana a quella predisposta dai Paesi aderenti alla Convenzione tecnologicamente più avanzati, quali, in particolare, Germania, Svezia, Regno Unito e Spagna.

La Convenzione di Budapest costituisce il primo esempio di accordo sovranazionale in materia di criminalità informatica, da intendersi come insieme di atti criminosi posti in essere tramite il mezzo informatico oppure rispetto ai quali le prove devono necessariamente essere raccolte in forma o in ambito telematico

[47] In particolare, questi sono i reati che sono stati introdotti dalla legge n. 547/1993: art. 615 *ter* c.p. "Accesso abusivo a un sistema informatico o telematico"; art. 615 *quater* c.p. "Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici", art. 615 *quinquies* c.p. "Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico", art. 617 *quater* c.p. "Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche", art. 617 *quinquies* c.p. "Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche"; art. 617 *sexies* c.p. "Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche", art. 635 *bis* c.p. "Danneggiamento di informazioni, dati e programmi informatici", art. 640 *ter* c.p. "Frode informatica".

o elettronico[48].

Per quanto concerne, in particolare, il profilo processuale, la Convenzione di Budapest ha avuto il merito di rendere più omogenei i diversi ordinamenti giuridici dei Paesi aderenti, garantendo uno sviluppo più armonico dei diversi istituti protesi a reprimere ed a prevenire la recrudescenza del fenomeno della criminalità informatica[49].

La cooperazione investigativa, fondamentale in generale per tutto il diritto penale, assume una rilevanza ancora maggiore per i reati informatici che sono spesso

[48] Come è stato osservato da Destito V., *Reati informatici*, cit., p. 143, «particolarmente significativo è stata, da parte della legge in questione ed in attuazione dell'art. 12 della Convenzione, l'estensione dei principi di responsabilità amministrativa degli enti nel caso di reati commessi nell'interesse o a vantaggio degli stessi (l. 8-6-2001, n. 231) ai reati informatici e, segnatamente, per le seguenti ipotesi delittuose: di cui agli artt. 491 bis (falsità in documenti informatici), 615 ter (accesso abusivo ad un sistema informatico o telematico), 615 quater (detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici), 615 quinquies (diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico), 617 quater (intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche), 617 quinquies (installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche), 635 bis (danneggiamento di informazioni, dati e programmi informatici), 635 ter (danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità), 635 quater (danneggiamento di sistemi informatici o telematici), 635 quinquies (danneggiamento di sistemi informatici o telematici di pubblica utilità) e 640 quinquies (frode informatica del soggetto che presta servizi di certificazione di firma elettronica) c.p. (cfr. art. 24 bis d.lg. n. 231/2001)».

[49] ROMANO B.N., *Il rischio di "attacchi" ai sistemi informatici tra fattispecie penalmente rilevanti, tutela dei dati ed esigenze di "buona amministrazione"*, in Amministrativ@mente, 3, 2021

espressione della nuova criminalità transfrontaliera. La criminalità organizzata transfrontaliera è, infatti, un tipo di criminalità che non è di per sé circoscritta in un singolo territorio geografico, ma si avvale di cellule sparse in tutto il mondo, compreso anche lo spazio cibernetico, che oggi assume delle dimensioni spropositate sia a causa dei mercati illeciti che gestisce, sia a causa della collaborazione di gruppi di diverse nazionalità ed etnie.

Orbene i reati informatici, per loro natura intrinseca, tendono sovente a valicare i confini tradizionali imposti dagli spazi fisici limitati: un soggetto che si trova davanti ad un PC in uno Stato, infatti, può andare a ledere gli interessi di un altro soggetto che si trova nella sua casa, davanti al suo PC, in un altro luogo situato dall'altra parte del mondo. Si aggiunga, poi, il fatto che, molto spesso, chi utilizza un PC per commettere un reato informatico utilizza un provider di un altro Stato al fine di non svelare la propria posizione geografica e non essere intercettato dagli investigatori[50].

Del resto, la globalizzazione e la digitalizzazione di messaggi e attività attraverso internet, meglio definito come cyberspazio, e la possibilità dell'anonimato, non consentono facilmente di individuare chi commette certi crimini che oggi possono essere perseguitati anche penalmente. Pare evidente, dunque, che la cooperazione investigativa nel settore dei reati informatici è decisiva se si vuole dare una risposta pronta ed immediata a tale nuovo settore della criminalità, cercando di prevenire il fenomeno o quantomeno di reprimerlo successivamente

[50] Cfr., sul tema, Mangiameli A.C., Saraceni G., *I reati informatici. Elementi di teoria generale e principali figure criminose*, Torino, Giappichelli, 2017, p. 15 ss.

in maniera efficace[51].

La prima fattispecie che tipizza delle condotte inconcepibili al di fuori del contesto informatico è quella relativa all'accesso abusivo a sistema informatico o telematico. Il delitto in questione è prodromico rispetto a numerose altre condotte delittuose nel *cyberspace.*

La collocazione sistematica piuttosto ambigua di tale disposizione rende piuttosto difficile individuare il bene giuridico tutelato nel caso in esame. Secondo una parte della dottrina, infatti, tale previsione, essendo stata inserita tra i reati contro il domicilio, sarebbe diretta a tutelare il c.d. domicilio informatico, ossia il luogo informatico all'interno del quale ciascuno è libero di esercitare qualunque attività informatica, senza subire intrusioni da parte di terzi. In altri termini, il domicilio informatico sarebbe l'equivalente "virtuale" del domicilio fisico[52].

Secondo questa interpretazione, quindi, il legislatore, mediante l'introduzione dell'art. 615 *ter* c.p., avrebbe optato per una estensione del domicilio e della tutela per esso normalmente prevista. Ne deriva che, in tale prospettiva, il domicilio informatico non potrebbe essere considerato a tutti gli effetti un nuovo bene giuridico, atteggiandosi, piuttosto, come mera specificazione del bene tradizionale del domicilio "fisico"[53].

---

[51] ROMANO B.N., *Il rischio di "attacchi" ai sistemi informatici tra fattispecie penalmente rilevanti, tutela dei dati ed esigenze di "buona amministrazione"*, in Amministrativ@mente, 3, 2021.

[52] Cfr., in tal senso, Alma M., Perroni C., *Riflessioni sull'attuazione delle norme a tutela dei sistemi informatici*, in *Diritto penale processuale*, 1997, p. 505.

[53] ROMANO B.N., *Il rischio di "attacchi" ai sistemi informatici tra fattispecie penalmente rilevanti, tutela dei dati ed esigenze di "buona amministrazione"*, in Amministrativ@mente, 3, 2021.

Questo orientamento è stato confermato anche da parte della giurisprudenza, secondo cui «con la previsione dell'art. 615 ter c.p., introdotto a seguito della l. 23 dicembre 1993, n. 547, il legislatore ha assicurato la protezione del "domicilio informatico" quale spazio ideale (ma anche fisico in cui sono contenuti i dati informatici) di pertinenza della sfera individuale, quale bene anche costituzionalmente protetto. Tuttavia l'art. 615 ter c.p. non si limita a tutelare solamente i contenuti personalissimi dei dati raccolti nei sistemi informatici protetti, ma offre una tutela più ampia che si concreta nello "ius excludendi alios", quale che sia il contenuto dei dati racchiusi in esso, purché attinente alla sfera di pensiero o all'attività, lavorativa o non, dell'utente; con la conseguenza che la tutela della legge si estende anche agli aspetti economico-patrimoniali dei dati sia che titolare dello jus excludendi sia persona fisica, sia giuridica, privata o pubblica, o altro ente»[54].

Secondo un diverso e prevalente orientamento[55], tuttavia, si tratterebbe di un'interpretazione inaccettabile, perché finirebbe con lo svalutare la nozione di domicilio informatico che non può essere ridotto a mero equivalente virtuale del domicilio fisico, perché in tal modo si finirebbe per estendere in maniera eccessiva la tutela penale, con il potenziale rischio di ledere i principi fondamentali del diritto penale[56].

---

[54] Cass. pen., 4 ottobre 1999, n. 3067, in *Cassazione penale*, 2000, p. 2990.

[55] Cfr., *ex multis*, Pazienza F., *In tema di criminalità informatica: l'art. 4 della legge 23 dicembre 1993, n. 547*, in *Rivista di diritto penale processuale*, 1995, p. 750

[56] ROMANO B.N., *Il rischio di "attacchi" ai sistemi informatici tra fattispecie penalmente rilevanti, tutela dei dati ed esigenze di "buona amministrazione"*, in Amministrativ@mente, 3, 2021

Secondo questa impostazione, dunque, il legislatore avrebbe commesso un errore nella collocazione sistematica dell'art. 615 ter c.p., giacché non assumono rilevanza «modalità di violazione dei luoghi di privata dimora bensì forme di offesa alla privacy che vengono ad interferire su strumenti capaci di favorire tecniche di lavoro intellettuale»[57].

Alla luce di queste considerazioni di carattere generale, si ritiene, dunque, che il bene giuridico tutelato dalla fattispecie in esame non sarebbe il domicilio fisico interpretato in maniera estensiva, bensì il diritto di godere in maniera indisturbata del sistema informatico: in particolare, si sostiene che, così come il proprietario di un fondo, ai sensi dell'art. 637 c.p., non deve essere disturbato da nessuno nel godimento del fondo stesso, allo stesso modo un proprietario di un sistema informatico non deve essere disturbato da nessuno nel godimento del sistema informatico[58].

Vi è, poi, anche un altro orientamento, secondo cui oggetto giuridico dell'art. 615 ter c.p. sarebbe la necessità di tutelare la *privacy*, ossia la riservatezza dei dati e dei programmi che si trovano all'interno del sistema informatico[59]. L'oggetto fisico della tutela, comunque, comune invero a tutti i reati informatici, è il sistema informatico che la giurisprudenza ha definito come «una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo,

---

[57] Merli A., *Il diritto penale dell'informatica: legislazione vigente e prospettive di riforma*, in *Giustizia penale*, 2, 1993, p. 127.

[58] Così Berghella F., Blaiotta R., *Diritto penale dell'informatica e beni giuridici*, in *Cassazione penale*, 1995, p.2330 ss.

[59] Cfr. Alma M., Perroni C., *Riflessioni sull'attuazione delle norme a tutela dei sistemi informatici*, cit., p. 505.

attraverso l'utilizzazione, anche in parte, di tecnologie informatiche, che sono caratterizzate - per mezzo di un'attività di "codificazione" e "decodificazione" - dalla "registrazione" o "memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "dati", cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit), in combinazioni diverse, e dalla elaborazione automatica di tali dati, in modo da generare "informazioni", costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente. Pertanto non lo è tutto ciò che, in un sito web o nel mondo dell'informatica, non è capace di gestire o elaborare dati in vista dello svolgimento di una funzione»[60].

La formulazione della norma incriminatrice richiama le condotte incriminate dal delitto di violazione di domicilio *ex* art. 614 c.p., in ragione dell'analogia che il legislatore del 1993 ravvisava tra il “domicilio informatico” e il domicilio fisico tradizionalmente inteso, la cui tutela sarebbe ugualmente fondata sull'art. 114 Cost.

Di conseguenza, il reato di accesso abusivo non soltanto presenta degli analoghi limiti edittali di beni, bensì si articola anche nelle due condotte dell’“introduzione” abusiva e del mantenimento (dopo un accesso illegittimo) contro la volontà del

[60] Così Trib. Milano, 19 marzo 2007, in *Diritto industriale*, 1, 2008, p. 85. I giudici di merito hanno escluso dunque il reato nel caso di riproduzione di dati di una banca dati contenuta in un sito non protetto da alcun sistema di sicurezza e in relazione al quale non risulta essersi verificata alcuna intrusione.

titolare dello *jus excludendi*[61].

La differenza di tali due ipotesi dal punto di vista strutturale è emersa sia con riguardo alla necessità di fornire una definizione di condotta di "introduzione" nel sistema – con la difficoltà di fissare il correlato *tempus* e *locus commissi delicti* – sia relativamente alla specifica delimitazione della condotta di "mantenimento" penalmente rilevante, successiva dal punto di vista logico ad un'introduzione autorizzata, la quale rimarrebbe altrimenti assorbita nell'accesso abusivo[62].

Le Sezioni Unite della Cassazione sono intervenute a chiarire tali profili.

Con riguardo al luogo di commissione, il Supremo Congresso ha stabilito che esso si identifica con il luogo in cui si trova l'autore che effettua l'accesso, introducendosi o mantenendosi nel sistema, e non invece con quello in cui si trova il *server* del sistema aggredito. Tuttavia, restano diverse perplessità concettuali e applicazione pratica, ampliate dal frequente ricorso a dispositivi mobili, i quali aumentano gli ostacoli per le attività investigative, non agevolando la tutela delle vittime[63].

A ben vedere, il momento in cui si consuma l'introduzione – non coincidente con quello di "accesso" - si può ravvisare soltanto laddove sia stato svolto un effettivo controllo informatico delle credenziali o delle azioni di accesso, che in rete

---

[61] ROMANO B.N., *Il rischio di "attacchi" ai sistemi informatici tra fattispecie penalmente rilevanti, tutela dei dati ed esigenze di "buona amministrazione"*, in Amministrativ@mente, 3, 2021.

[62] ROMANO B.N., *Il rischio di "attacchi" ai sistemi informatici tra fattispecie penalmente rilevanti, tutela dei dati ed esigenze di "buona amministrazione"*, in Amministrativ@mente, 3, 2021.

[63] PERRI P., *Analisi informatico-giuridica delle più recenti interpretazioni giurisprudenziali in tema di phishing*, in *Ciberspazio e Diritto*, 1, 2008.

avviene mediante la connessione telematica tra il terminale e il *server*, presso il quale ultimo soltanto può dirsi perfezionata l' “introduzione”, come fase finale della procedura, distinta dalla previa mera immissione dei dati, che ancora non implica alcun effettivo trattamento automatizzato, operato dal sistema nell'ambito degli spazi informatici di cui è titolare la vittima.

Circa la condotta di “mantenimento”, essa può assumere rilievo penale soltanto laddove violi – successivamente all'introduzione – le regole e le disposizioni dell'avente diritto, in merito alle azioni che si possono porre in essere in tali spazi informatici.

Pertanto, dal punto di vista della tecnologia informatica, tale attività si svolge nel luogo nel quale è posto il *server* e non nel luogo in cui è posto invece il terminale periferico da cui vengono soltanto immessi i dati[64].

Si può dire che la norma in questione punisce ogni oggettiva violazione dell'esclusiva disponibilità degli spazi informatici cui ha diritto il titolare (c.d. *jus ecludendi alios*), poiché instaura un rapporto conflittuale apprezzabile con riguardo non soltanto alle procedure informatiche che abilitano e legittimano l'introduzione e l'utilizzo del sistema, ma anche in merito alle regole e alle disposizioni generali, sebbene non propriamente informatiche, aventi un contenuto precettivo, poste dal titolare del sistema o a lui riferibili anche al fine di regolare il successivo mantenimento in tali spazi, da considerare *contra jus* qualora in contrasto con la sua volontà[65]. Quest'ultima non deve essere intesa in

---

[64] PERRI P., *Analisi informatico-giuridica delle più recenti interpretazioni giurisprudenziali in tema di phishing*, in *Ciberspazio e Diritto*, 1, 2008.

[65] PERRI P., *Analisi informatico-giuridica delle più recenti interpretazioni giurisprudenziali in tema di phishing*, in *Ciberspazio e Diritto*, 1, 2008.

meri termini psicologici o soggettivi, essendo difficile concepire e riconoscere in capo ad un ente o ad un'amministrazione, quanto sul piano oggettivo delle regole e disposizioni con cui viene ad esternarsi, che sono anche integrare indirettamente dalla disciplina delle competenze e delle attività d'ufficio, come avviene nel caso delle organizzazioni complesse, sia private che pubbliche, la cui violazione integra il requisito dell'abuso di poteri o della violazione dei doveri, rappresentando un elemento normativo extrapenale che completa la tipizzazione del fatto oggettivo costitutivo del reato[66].

Anche il delitto di "*diffusione di apparecchiature dirette a danneggiare un sistema informatico o telematico" ex* art. 615 *quinquies* c.p. ha rappresentato, al pari di quello di cui all'art. 615 *quater* c.p., una novità in ambito europeo[67].

Ed invero, l'art. 615 *quinquies* c.p. punisce un'ampia gamma di condotte preparatorie alla commissione dei reati di danneggiamento di dati, di informazioni o programmi informatici (artt. 635 *bis* e 635 *ter* c.p.), ovvero di sistemi informatici o telematici (artt. 635 *quater* e 635 *quinquies* c.p.).

Contrariamente quanto previsto dall'art. 615 *quater*, il legislatore degli anni Novanta aveva punito in origine soltanto le condotte finalizzate a "far entrare" i c.d. *malware* nella sfera altrui ("*diffonde*", "*comunica*", ovvero "*consegna*").

Con la Legge n. 48/2008 – con la quale è stata ratificata e data esecuzione alla Convenzione *Cybercrime* – è stata modificata la formulazione della norma in

---

[66] PERRI P., *Analisi informatico-giuridica delle più recenti interpretazioni giurisprudenziali in tema di phishing*, in *Ciberspazio e Diritto*, 1, 2008.

[67] PERRI P., *Analisi informatico-giuridica delle più recenti interpretazioni giurisprudenziali in tema di phishing*, in *Ciberspazio e Diritto*, 1, 2008.

questione, con il proposito di adeguarla agli *standard* sovranazionali[68].

L'opportuna estensione dell'ambito delle condotte penalmente rilevanti a quelle finalizzate a far entrare i predetti *malware* nella sfera di signoria del soggetto agente ("*si procura*", "*produce*", "*riproduce*", "*importa*") ha reso la formulazione della previsione legale omogenea rispetto a quella di cui all'art. 615 *quater* c.p.

Successivamente alle modifiche legislative operate con l'intervento di riforma del 2008, le condotte tipiche devono avere quale oggetto "*apparecchiature, dispositivi o programmi informatici"*.

Tuttavia, non viene richiesto che questi ultimi siano "*principalmente adattati o disegnati"* al fine di commettere un reato informatico contro l'esclusiva disponibilità ed integrità di dati o di sistemi informatici.

In assenza di ogni riferimento all'intrinseca dannosità o pericolosità dei "dispositivi" che devono essere oggetto delle condotte di procurarsi, produrre, diffondere, importare, distribuire o cedere, il contenuto dell'offesa oggetto della norma viene ricavato in modo discutibile soltanto sul fine illecito, il quale deve sorreggere il fatto-base[69].

Tuttavia, in tal modo è stata tipizzata una condotta altrimenti priva di offensività autonoma oggettiva[70].

Ed invero, il delitto è punibile soltanto a titolo di dolo specifico, poiché le condotte

---

[68] MODESTI G., *Il reato di frode informatica. Una rilettura alla luce delle recenti traiettorie giurisprudenziali*, in *Ragiusan*, 335-337, 2012.

[69] MODESTI G., *Il reato di frode informatica. Una rilettura alla luce delle recenti traiettorie giurisprudenziali*, in *Ragiusan*, 335-337, 2012.

[70] MODESTI G., *Il reato di frode informatica. Una rilettura alla luce delle recenti traiettorie giurisprudenziali*, in *Ragiusan*, 335-337, 2012.

“neutre” che si sostanziano nell'esercizio di una signoria ovvero nel mettere a disposizione di terzi apparecchiature, dispositivi o programmi informatici, rispetto ai quali non viene richiesta alcuna qualificazione intrinseca di dannosità, devono essere sorrette dal fine specifico di creare un danno illecito ad un sistema informatico o telematico, oppure ai dati in esso contenuti o ancora di favorire l'interruzione, totale o parziale, o l'alterazione del funzionamento di un sistema informatico o telematico[71].

Occorre precisare che in alcune ipotesi – a differenza di quanto si è visto per i delitti di accesso abusivo a sistema informatico o telematico e i reati prodromici – il legislatore non ha provveduto ad inserire nuove fattispecie incriminatrici, bensì si è limitato a ridefinire o ad aggiungere a fattispecie già esistenti, oggetti passivi o materiali “nuovi”, ovvero alcune nuove modalità di svolgimento della condotta, secondo un criterio di analogia che fa diretto rinvio ad esse o ne riproduce gli elementi essenziali, come è avvenuto per il delitto di danneggiamento di dati e sistemi informatici *ex* art. 635 *bis* c.p., introdotto nel 1993 e poi riformulato nel 2008, con la previsione di quattro distinte fattispecie incriminatrici.

Esemplare in tal senso è la tutela della corrispondenza informatica. Il legislatore del 1993, aggiungendo all'art. 616 c.p. un quarto comma ha stabilito che: “*agli effetti delle disposizioni di questa sezione, per corrispondenza si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza”*.

[71] MORGANTE G., *Il reato come elemento del reato. Analisi e classificazione del concetto di reato richiamato dalla fattispecie penale,* Torino, p. 58.

Pertanto, il legislatore, non ha utilizzato una definizione specifica dell'oggetto materiale delle condotte punibili (come avvenuto con riguardo ai delitti di falsità in documenti informatici di cui all'art. 491 *bis* c.p., come introdotto nel 1993, poi riformulato nel 2008), ma ha soltanto esteso l'applicabilità di tutte le fattispecie in materia di corrispondenza alle nuove forme di comunicazione, chiudendo l'elencazione con una formula aperta all'evoluzione tecnologica futura ("*ogni altra forma..."*), talmente indeterminata da rischiare di consentire estensioni analogiche in *malam partem*, le quali possono essere evitate soltanto circoscrivendo il *genus* cui possono essere ricondotte le varie *species*, ivi comprese quelle non ancora espressamente denominate o disciplinate dal legislatore[72].

Si tratta di operazione non certo agevole, stante la particolarità e varietà delle nuove forme telematiche di comunicazione[73], le quali coinvolgono in maniera attiva un possibile numero di destinatari, consentendone la circolazione nell'ambito di gruppi, reti sociali, *chat* aperte, aventi un'estensione variabile e talvolta, addirittura, indeterminata[74].

L'art. 9, comma 1, lett. a), della Legge 15 ottobre 2013, n. 119 – che ha convertito in legge, con modificazioni, il Decreto Legge 14 agosto 2013, n. 93, "*recante disposizioni urgenti in materia di sicurezza e per il contrasto della violenza di*

---

[72] PICOTTI L., *Commento art. 5 L. 23.12.1993, n. 547 (art. 616, comma 4, c.p.),* in *Leg. Pen.,* 1996, p. 109.

[73] MODESTI G., *Il reato di frode informatica. Una rilettura alla luce delle recenti traiettorie giurisprudenziali*, in *Ragiusan*, 335-337, 2012.

[74] MODESTI G., *Il reato di frode informatica. Una rilettura alla luce delle recenti traiettorie giurisprudenziali*, in *Ragiusan*, 335-337, 2012.

genere, nonché in tema di protezione civile e di commissariamento delle province – ha inserito nell'art. 640 *ter* c.p. ("frode informatica"), un nuovo comma, il quale sanziona la frode informatica posta in essere mediante sostituzione (furto o indebito utilizzo) "*dell'identità digitale in danno di uno o più soggetti".*

Dal punto di vista della collocazione sistematica, parte della dottrina[75] ha ritenuto che si tratti di una circostanza aggravante della frode sistematica, ritenendo che, poiché la norma utilizza l'espressione "*se il fatto è commesso con"*, piuttosto che procedere ad una sua nuova descrizione o all'uso di una locuzione quale "*se il fatto consiste in"*, essa rinvia necessariamente al contenuto tipizzato nell'ipotesi-base prevista dal primo comma dell'art. 640 *ter* c.p.[76].

1.5.1 Lo sviluppo tecnologico e la mancanza di una norma *ad hoc*

L'evoluzione accelerata delle tecnologie digitali ha reso più difficile la definizione di norme e regolamenti specifici che possano tenere il passo con i cambiamenti. Questa situazione è particolarmente evidente in settori come l'Internet delle cose (IoT), l'intelligenza artificiale (IA), la blockchain e altre tecnologie emergenti. La mancanza di una normativa chiara in questi settori può avere una serie di implicazioni profonde.

Innanzitutto, le organizzazioni si trovano spesso ad affrontare un terreno instabile quando cercano di stabilire politiche e procedure di sicurezza informatica. Senza

[75] MALGIERI L., *La nuova fattispecie di indebito utilizzo di identità digitale: un problema interpretativo,* in *Dir. Pen. Cont.,* 2015, n. 2, p. 143.

[76] *Ibidem.*

linee guida chiare, è difficile per le aziende proteggere in modo efficace le proprie reti e i dati sensibili. Questo può portare a vulnerabilità crescenti e a un aumento degli incidenti di sicurezza informatica[77].

Le violazioni dei dati sono diventate una preoccupazione sempre più rilevante, e la mancanza di norme specifiche può esporre le aziende a rischi significativi in termini di responsabilità legale e danni alla reputazione. Inoltre, il pubblico in generale può essere colpito da una mancanza di regolamentazione, rendendo le persone più vulnerabili a frodi online e altri crimini informatici.

L'aspetto internazionale della questione è altrettanto importante. Poiché le minacce informatiche spesso attraversano le frontiere, la mancanza di norme internazionali può ostacolare la cooperazione tra paesi nell'identificare e perseguire i responsabili di attacchi informatici.

Per affrontare queste sfide, è necessario promuovere un dialogo interdisciplinare tra governi, organizzazioni private, accademici e organizzazioni internazionali. Questo può contribuire a sviluppare normative flessibili che possano essere aggiornate rapidamente per far fronte alle nuove minacce. È essenziale anche investire nella ricerca e sviluppo per identificare e mitigare le minacce emergenti e promuovere la consapevolezza sulla sicurezza informatica tra il pubblico e le aziende.

In sintesi, la mancanza di norme *ad hoc* in un contesto di sviluppo tecnologico rapido è una sfida significativa per la sicurezza informatica e la protezione dei

[77] FRAU R., *"Home banking", captazione di credenziali di accesso dei clienti tramite "phishing" e responsabilità della banca*, in *Responsabilità civile e previdenza*, 3, 2015, p. 125 ss.

dati. Affrontare questa sfida richiede un approccio collaborativo, flessibilità normativa e un impegno a livello internazionale per proteggere la privacy e la sicurezza nel mondo digitale in continua evoluzione[78].

Pare ora opportuno soffermarsi, in particolare, sul phishing, che costituisce probabilmente la massima espressione sul cybercrime.

[78] FRAU R., *"Home banking", captazione di credenziali di accesso dei clienti tramite "phishing" e responsabilità della banca*, in *Responsabilità civile e previdenza*, 3, 2015, p. 129 s.

CAPITOLO II
Il phishing et similia: l'evoluzione dei reati informatici

2.1 Profili generali e inquadramento del fenomeno

Il termine *phishing* deriva dal termine anglosassone "*fhishing"* - letteralmente "pescare" - di cui rappresenta una variabile[79].

Tale concetto è entrato ormai a far parte del linguaggio criminologico moderno, consistendo in una tecnica fraudolenta diretta a carpire delle informazioni personali e sensibili, come dati anagrafici, *user ID*[80] e *password*[81] per accedere ai conti correnti *online*, codici di carte di credito, facendo leva sugli aspetti c.d. sociali di *internet*.

Tutto ciò al fine di commettere degli illeciti bancari attraverso il *web*, accedendo ai sistemi di *home banking*[82] o a conti correnti e servizi *online* per effettuare operazioni e bonifici attuati in frode ai titolari.

In altre parole, il *phishing* può essere definito come una tecnica di *social engineering*[83] che, attraverso l'invio di *e-mail* ingannevoli da parte dei truffatori,

---

[79] A. Cadoppi, S. Canestrari, A. Manna, M. Papa, *Cybercrime*, Padova, 2023, p. 907 ss.

[80] Per *user ID* si intende il nome con cui ci si registra al sito, letteralmente: identità dell'utente, può combaciare con la propria mail o con un nome di propria scelta.

[81] Per *password* si intende una "parola" in codice e segreta, che viene scelta per accedere al sito, solitamente trattasi di parole da minimo 8 carattere, una maiuscola, e viene richiesto di inserire un numero e un carattere speciale: !?%&$

[82] Per *home banking* si intende la possibilità di accedere al proprio conto online e compiere operazioni finanziarie con lo stesso (bonifici, pagamenti MAV, F24, bollettini pagoPA ecc) senza recarsi in filiale.

[83] Il social engineering, o ingegneria sociale, riguarda sostanzialmente la psicologia della persuasione. In buona sostanza, altro non è che l'evoluzione digitale degli artifizi e raggiri tipici delle truffe. L'obiettivo è guadagnare la fiducia degli utenti, così che abbassino la guardia, e poi incoraggiarli a compiere azioni non sicure, come divulgare informazioni personali, fare clic sui link oppure aprire allegati che possono essere dannosi.

porta le vittime a fornire volontariamente delle informazioni e dati di carattere personale, riguardanti soprattutto le credenziali di autenticazione per accedere alle aree informatiche personali o a servizi bancari *online*, numeri di carte di credito, identificativi per le abilitazioni all'accesso a siti di vario genere, numero di conto corrente, numero ed estremi della carta di identità, della patente, assumendo virtualmente l'identità del legittimo titolare o utente[84].

In buona sostanza, la frode si concretizza nell'invio casuale di messaggi di posta elettronica ad alto numero di destinatari[85] che sembrano provenire da enti, istituti o società reali, aventi ad oggetto messaggi, immagini ed informazioni appositamente formulati in modo tale da influenzare la psiche del destinatario il quale, di fronte al ricevimento di tali comunicazioni, viene spinto a collegarsi a diverse pagine *web,* non autentiche ma analoghe a quelli delle citate istituzioni o enti, e ad inserire le proprie credenziali per l'accesso ad aree riservati, servizi *online*, in particolare l'*home banking*, cliccando sui *link* o sui *form*[86] creati *ad hoc* dal *phisher*, ovvero operando un collegamento *ex novo* dal proprio terminale, già infettato da un *trojan*[87]*.*

Il fenomeno in questione ha iniziato a diffondersi alla fine del secolo scorso e, attualmente, la tecnica ha avuto larga diffusione, non limitandosi al

---

[84] FLOR F., *Phishing, identify theft e identify abuse: le prospettive applicative del diritto penale vigente,* in *RIDPP,* 2007, p. 899. Secondo l'autore la diffusione del fenomeno phishing, solo fino a pochi anni fa sconosciuto in Italia, ha messo in risalto i problemi di adeguamento del diritto penale positivo rispetto agli abusi dei "profili identitari" nel cyberspace, che nell'odierna "epoca di Internet" diviene l'ambiente ideale per la realizzazione di molteplici forme di reati.

[85] La tecnica in questione è denominata *spamming*.

[86] Per *form* si intendono i moduli

[87] La tecnica menzionata è denominata *pharming.*

perseguimento di un lucro di carattere pecuniario, ma investendo anche in tecniche e forme più sofisticate, tali da mettere a rischio di settori della *cybersecurity*, dei servizi finanziari e della tutela dei consumatori[88].

In un primo momento, il fenomeno del *phishing* era generato, in via principale, dall'invio massivo di e-mail e diffuso soprattutto negli Stati dell'America del Nord; successivamente, tale tecnica trovò diffusione anche in altri Paesi – tra cui l'Italia – la quale ha subito il primo attacco in tal senso nel marzo 2005, mediante una serie di *e-mail* ingannevoli inviate ai clienti di Poste Italiane.

Da quel momento, si è diffuso sempre più l'invio di *e-mail* riferite ad istituti di credito nazionali, tanto che l'Italia ha iniziato ad assumere un ruolo sempre più importante nella classifica delle nazioni con maggior numero di istituti bancari colpiti da tali attacchi[89]

In tal senso, si possono prendere in considerazione i *report* resi noti dall'osservatorio *Anti-Phishing* Italia, promosso da uno *staff* formato da giornalisti, informatici, avvocati, aperto a collaborazioni esterne[90].

Più nel dettaglio, nei primi mesi dell'anno 2007 (da gennaio a marzo), sono stati rilevati ben 225 tentativi di *phishing*, con una media di 2,5 attacchi al giorno: si trattava di un dato alquanto preoccupante, in considerazione del fatto che, nello stesso periodo dell'anno precedente, il numero totale di attacchi era stato di soli

---

[88] MASSA R.G., *Il phishing,* 2008, *http://www.pmi.it/impresa/normativa/articolo/1999/il-phishing.html*

[89] *Ibidem.*

[90] FRAU R., *"Home banking", captazione di credenziali di accesso dei clienti tramite "phishing" e responsabilità della banca*, in *Responsabilità civile e previdenza*, 3, 2015, p. 125 ss.

12 e, nel solo mese di gennaio del 2006, il numero di attacchi era pari a zero[91].

Nel secondo trimestre del 2007, vi fu un ulteriore aumento degli attacchi, i quali salirono del 90% rispetto al primo trimestre.

Ad essere maggiormente colpita fu la società Poste Italiane – con una frequenza di due attacchi al giorno – probabilmente in ragione del fatto che i conti Banco Posta e le carte prepagate Poste Pay erano particolarmente diffuse ed utilizzate per gli acquisti sul *web*; seguiva poi Banca Intesa, con una percentuale di attacchi pari al 6% e il sito di aste *online* eBay.

Nel corso degli anni, il numero degli attacchi di *phishing* si è moltiplicato: difatti, negli anni 2014-2015, fu particolarmente elevato il numero di attacchi registrato, rilevandosi anche l'utilizzo di numerose piattaforme per espletare tali attacchi, ovvero i *social network*, come *Facebook* e Twitter[92].

Pertanto, gli attacchi tramite la tecnica del *phishing* sono in crescita repentina e, al fine di comprendere la reale dimensione del fenomeno a livello mondiale,

---

[91] G. Aronica, *Il "fishing" tra nuove esigenze di tutela ed acrobazie interpretative della giurisprudenza*, in Il *Foro ambrosiano*, 2008, pp. 74-85.

[92] PICOTTI L., *I diritti fondamentali nell'uso e abuso dei social network. Aspetti penali,* in *Giur. Merito,* n. 12, 2012, p. 2522. Secondo l'autore occorre rivedere le categorie dogmatiche dei vari campi del diritto alla luce delle incessanti novità tecnologiche, che non sono solo tecniche, ma anche sociali, economiche, politiche, culturali, di vita personale, è essenziale sapere come il diritto abbia via via cercato di adattarsi a questa evoluzione, per ricavarne indicazioni utili all'ulteriore sviluppo e qualche warning su errori da non ripetere. Se Internet, o – meglio – il cyberspace è divenuto uno spazio reale, strettamente intrecciato con la vita nostra e della collettività, ha posto problemi nuovi al giurista. Basti pensare, nel campo penale, al momento consumativo ed al luogo di commissione del reato: il tempus commissi delicti, il locus commissi delicti, che sono categorie basilari di grande rilievo anche per la disciplina e l'applicazione concreta della legge penale, dovendosi prioritariamente stabilire quando e dove il reato si perfeziona nei suoi elementi essenziali, che integrano una fattispecie incriminatrice, ed anche quando se ne esauriscano gli effetti offensivi, e dove e come questo avvenga.

considerando anche il fatto che alcuni tentativi di *phishing* non sono rilevati, si può considerare l'analisi dei *Phishing Activity Trends Reports,* elaborati dall'*Anti Phishing Working Group*[93].

I risultati dei *report* mostrano, in particolare, un aumento del fenomeno sia con riguardo ai casi segnalati, sia con riguardo al numero dei nuovi siti di *phishing*. Il settore maggiormente colpito dagli attacchi resta quello dei servizi finanziari, mentre il Paese che ospita il maggior numero di *host* è gli Stati Uniti d'America, seguiti da Corea, Cina e Germania.

La durata minima e massima di vita di un *phishing site* è rilevante in quanto varia da un minimo di 4 ad un massimo di 27 giorni, elemento che inevitabilmente incide sul piano dell'accertamento del fatto e dell'individuazione del suo autore[94].

2.2 Le fasi del *phishing attack*

La tecnica degli attacchi si articola in sei fasi, le quali mirano a conseguire lo scopo avuto di mira dal *phishing,* ovvero il furto di informazioni e dati personali dell'utente[95].

La prima fase è quella del *planning,* ovvero quella in cui il *phisher*, ovvero l'attaccante, determina l'obiettivo da colpire e le tecniche da utilizzare in tal senso.

---

[93] L'*Anti Phishing Working Group* è stato fondato nel 2003 da David Jevans al fine di creare un consorzio internazionale, il quale, ad oggi, conta più di 3000 membri, formato da aziende *leader* nel campo della sicurezza informatica e finanziaria per tutelare da attacchi di *phishing*.

[94] CAJANI F., *Profili penali del phishing*, in *CP*, 2007, p. 2294.

[95] F. CAJANI, G. COSTABILE, G. MAZZARACO, *Phishing e furto d'identità digitale. Indagini informatiche e sicurezza bancaria*, Milano, 2008, p. 13 ss.

In seguito, egli si adopera a configurare i *tools* e i meccanismi occorrenti per poter sferrare l'attacco, ricercando anche delle informazioni utili sulle potenziali vittime. In tal modo si passa alla seconda fase, ovvero quella del "*Setup*".

La fase dell'attacco vero e proprio è la cosiddetta fase di "attacco", in cui l'attaccante inizia a stabilire un contatto con le potenziali vittime, sfruttando tutti i tipi di strumenti messi a disposizione dalla rete, come e-mail, dialer, newsgroup, messaggistica istantanea, chat, siti Web, software dannoso e bacheche elettroniche.

Tale contatto presenta l'obiettivo di spingere le vittime a compiere azioni che possano portarlo a conoscere le loro credenziali, in modo da passare alla fase c.d. "*collection*", nella quale l'attaccante sottrae realmente ed effettivamente le credenziali alle vittime.

Lo scopo di questo collegamento è incoraggiare le vittime ad agire e far loro conoscere le proprie credenziali per entrare nella cosiddetta fase di "raccolta", in cui l'attaccante sottrae effettivamente ed efficacemente le credenziali della vittima[96].

Dopo aver sottratto le credenziali di accesso, l'attaccante conduce la vera e propria attività fraudolenta: si tratta della fase di "frode", in cui le credenziali vengono utilizzate per acquistare beni, rubare identità o riciclare denaro[97].

Infine, la fase finale rappresentata dal "post attacco", in cui l'attaccante, dopo aver

---

[96] FRAU R., *"Home banking", captazione di credenziali di accesso dei clienti tramite "phishing" e responsabilità della banca*, in *Responsabilità civile e previdenza*, 3, 2015, p. 125 ss.

[97] G. D'AIUTO, L. LEVITA, *I reati informatici. Disciplina sostanziale e questioni processuali*, Milano, 2012, p. 18 s.

raggiunto il suo scopo fraudolento, compie qualsiasi azione per coprire le proprie tracce e disabilitare i meccanismi attraverso i quali ha potuto svolgere l'attività fraudolenta, verifica anche il successo dell'attacco e inizia a pianificare l'attacco successivo[98].

2.2.1 Modalità di attuazione e misure tecniche

Il phishing, come si è visto, è una forma di attacco informatico che mira a ingannare le vittime per ottenere informazioni sensibili, come username, password, dati finanziari o altre informazioni personali. Esistono diverse modalità di attuazione del phishing, insieme a misure tecniche che possono essere adottate per prevenirlo o rilevarlo[99].

Modalità di Attuazione del Phishing:

1. **Phishing via Email**: Gli hacker inviano email che sembrano provenire da fonti affidabili, come banche, servizi online o aziende. Le email contengono spesso link malevoli o allegati dannosi.

   Contromisure: Verifica attentamente l'indirizzo email del mittente, non cliccare su link sospetti o scaricare allegati da mittenti non attendibili. Usa filtri antispam per rilevare e bloccare email di phishing.

2. **Phishing via SMS (Smishing)**: Simile al phishing via email, ma coinvolge

[98] CAJANI F., COSTABILE G., MAZZARACO G., *Phishing e furto di identità digitale. Indagini informatiche e sicurezza bancaria,* Milano, 2008, p.16.

[99] FRAU R., *"Home banking", captazione di credenziali di accesso dei clienti tramite "phishing" e responsabilità della banca*, in *Responsabilità civile e previdenza*, 3, 2015, p. 125 ss.

messaggi di testo su dispositivi mobili.

Contromisure: Non rispondere a messaggi di testo sospetti o con link non verificati. Utilizza app antiphishing per proteggerti dai messaggi di phishing.

3. **Phishing via Chiamate Telefoniche (Vishing)**: Gli hacker chiamano le vittime fingendo di essere un'entità legittima, come un'istituzione finanziaria o un'azienda, per ottenere informazioni personali.

   Contromisure: Non condividere informazioni sensibili tramite telefonate inaspettate. Verifica l'identità del chiamante e cerca informazioni di contatto ufficiali per confermare la richiesta[100].

4. **Phishing via Siti Web Fraudolenti**: Gli hacker creano siti web contraffatti che imitano quelli legittimi, spesso per rubare credenziali di accesso.

   Contromisure: Controlla attentamente l'URL del sito web. Utilizza sempre connessioni sicure HTTPS e assicurati che il sito sia autentico prima di inserire informazioni sensibili.

5. **Phishing Social Engineering**: Gli hacker utilizzano informazioni personali o di contatto reperite online (ad esempio dai social media) per creare messaggi di phishing altamente personalizzati[101].

[100] FIORIGLIO G., Sorveglianza e controllo nella società dell'informazione. il possibile contributo dell'etica hacker, in Nomos. Le attualità del diritto. Quadrimestrale di teoria generale, diritto pubblico comparato e storia costituzionale 2, 2014.

[101] FIORIGLIO G., Sorveglianza e controllo nella società dell'informazione. il possibile contributo dell'etica hacker, in Nomos. Le attualità del diritto. Quadrimestrale di teoria generale, diritto pubblico comparato e storia costituzionale 2, 2014.

Contromisure: Mantieni le tue informazioni personali private sui social media. Fai attenzione a messaggi che sembrano troppo personali o che richiedono informazioni che non dovrebbero essere conosciute dall'altra parte[102].

Misure Tecniche per Prevenire e Rilevare il Phishing:

1. **Filtraggio Antispam**: Utilizza filtri antispam avanzati per bloccare le email di phishing in arrivo.
2. **Certificati SSL**: Assicurati che i siti web utilizzino connessioni sicure HTTPS e verifica i certificati SSL.
3. **Autenticazione Multi-fattore (MFA)**: Abilita l'MFA per account online quando possibile, poiché rende più difficile per gli hacker accedere ai tuoi account anche se ottengono le tue credenziali.
4. **Educazione degli Utenti**: Fornisci formazione e sensibilizzazione agli utenti sul riconoscimento e la prevenzione del phishing.
5. **Utilizzo di Soluzioni Antiphishing**: Impiega strumenti e servizi di sicurezza antiphishing che possono rilevare e segnalare potenziali minacce.
6. **Aggiornamenti Software**: Mantieni il tuo sistema operativo e il software antivirus aggiornati per proteggerti da vulnerabilità conosciute.
7. **Monitoraggio dell'Attività Anomala**: Monitora l'attività degli account online alla ricerca di comportamenti sospetti.

---

[102] FIORIGLIO G., *Sorveglianza e controllo nella società dell'informazione. il possibile contributo dell'etica hacker*, in *Nomos. Le attualità del diritto. Quadrimestrale di teoria generale, diritto pubblico comparato e storia costituzionale* 2, 2014.

2.3 Le tipologie di *phishing*

La tipologia di *phishing* più comune è quella del "*deceptive phishing*", ovvero il *phishing* ingannevole, che si realizza quando l'attaccante invia ad un elevato numero di potenziali vittime un messaggio *e-mail* ingannevole, con invito a cliccare su un collegamento *web*.

In questo modo la vittima viene reindirizzata ad un sito *web* che consente a quest'ultimo soggetto di raccogliere dei dati riservati relativi all'utente, al fine poi di effettuare un furto della sua identità per trasferire denaro, effettuare acquisti di beni o danneggiare in qualsiasi altro modo[103].

In diversi casi, il *phisher* non provoca direttamente un danno economico alla propria vittima, bensì rivende su un mercato secondario le informazioni e i dati che ha carpito in maniera fraudolenta, attraverso dei *forum* di mediante *online*[104].

Vi sono diverse varianti di *phishing* ingannevole: ad esempio, si può presentare una replica della pagina di *login* a chi legge i messaggi in formato HTML direttamente dal testo del messaggio di posta elettronica, in modo tale non si ponga la necessità di cliccare su un collegamento ad un sito *web*. Ancora, si può utilizzare un indirizzo IP numerico al posto del nome dell'*host* nella stringa di collegamento ad un sito di *phishing*, in modo tale che, per prendere il controllo della barra degli indirizzi di un *browser,* debba essere utilizzato *Javascript* oppure

---

[103] FIORIGLIO G., *Sorveglianza e controllo nella società dell'informazione. il possibile contributo dell'etica hacker*, in *Nomos. Le attualità del diritto. Quadrimestrale di teoria generale, diritto pubblico comparato e storia costituzionale* 2, 2014.

[104] G. D'AIUTO, L. LEVITA, *I reati informatici. Disciplina sostanziale e questioni processuali*, cit., p. 18 ss.

vi sia bisogno di ingannare in altro modo l'utente facendogli credere che sta comunicando con un sito legittimo[105].

Inizialmente, le *e-mail* fraudolente venivano inviate in lingua inglese; con il passare del tempo venivano inviate in un italiano sempre più corretto, prendendo a modello una reale comunicazione di servizio della società, imitandone alla perfezione non solo la rappresentazione grafica del messaggio, bensì anche il linguaggio adoperato.

Facendo click sul *link* contenuto nel testo del messaggio di posta, la pagina caricata non è quella del sito della società o dell'ente, bensì un sito *web* fittizio, creato dal *phisher* al fine di sottrarre e memorizzare le informazioni fornite dagli utenti ignari[106].

Pertanto, possono essere inviate, da parte del *phisher:* dei messaggi *e-mail* che invitano ad effettuare l'accesso sul sito della propria banca per ottenere il codice pin di sicurezza; delle *e-mail* contenenti un avviso di addebito sul conto di un importo elevato e la richiesta di fare *click* su un link per ottenere *user ID* e *password* dell'utente; delle *e-mail* che invitano ad accedere alla propria banca proprio in quanto dei presunti *phishers* avrebbero attentato alla sicurezza del conto corrente dell'utente per raccogliere i dati digitali della vittima ed inviarli ad

[105] FIORIGLIO G., *Sorveglianza e controllo nella società dell'informazione. il possibile contributo dell'etica hacker*, in *Nomos. Le attualità del diritto. Quadrimestrale di teoria generale, diritto pubblico comparato e storia costituzionale* 2, 2014.

[106] G. D'AIUTO, L. LEVITA, *I reati informatici. Disciplina sostanziale e questioni processuali*, cit., p. 43 ss.

un *hacker*[107].

Ciò fa comprendere come il fenomeno in questione stia ormai dilagando, anche grazie all'utilizzo di *virus* per carpire delle informazioni riservate sui conti bancari o per dirottare gli utenti su dei veri e propri siti-clone nel momento in cui si digita il sito *web* del proprio istituto bancario[108].

Altra tipologia di *phishing attack* è quello basato su *malware*: con tale espressione si fa riferimento ad un tipo di attacco, il quale richiede di eseguire sul *computer* dell'utente, a sua insaputa, un *software* utilizzando inganni di *social engineering* oppure sfruttando le vulnerabilità del sistema di sicurezza[109].

Un tipico inganno in tal senso è quello di convincere l'utente ad aprire l'allegato di un'*e-mail* oppure di scaricare un *file* da un sito *web*, sostenendo che esso sia di carattere pornografico, oppure contenente informazioni di *gossip* su personaggi famosi; oppure si tratta di *software* scaricabili da internet, i quali possono contenere un codice maligno, il quale può essere diffuso mediante attacchi alla sicurezza, sia mediante la propagazione di *worm* o *virus* che approfittano di una vulnerabilità del sistema per installare il codice maligno, sia rendendo disponibile il codice in questione su di un sito che sfrutta una vulnerabilità di sicurezza[110].

Tale tipologia di *phishing* fondato sul codice maligno può assumere diverse

---

[107] FIORIGLIO G., *Sorveglianza e controllo nella società dell'informazione. il possibile contributo dell'etica hacker*, in *Nomos. Le attualità del diritto. Quadrimestrale di teoria generale, diritto pubblico comparato e storia costituzionale* 2, 2014.

[108]La tecnica in questione è denominata *hijacking*.

[109] G. D'AIUTO, L. LEVITA, *I reati informatici. Disciplina sostanziale e questioni processuali*, cit., p. 60 ss.

[110]Si tratta della tecnica del c.d *cross-site scripting*.

forme:

- quella dei “dirottatori di sistema” (c.d. *session hijacking*), ovvero quell'attacco mediante il quale si monitorano le attività di un utente – di solito mediante una componente non legittima del *browser* – per cui, quando egli inserisce le proprie credenziali di accesso di un *account*, o effettua una transazione, il *software* trasferisce la sessione per eseguire le attività necessarie alla frode[111];

- quella dei cavalli di troia sul *web* (c.d. *web trojans*), vale a dire dei programmi che si agganciano agli schermi di login per prelevare le credenziali di accesso, per cui l'utente crede di inserire i propri dati su un certo sito *web* ma in realtà i dati sono immessi localmente e trasferiti al *phisher* per un utilizzo fraudolento degli stessi;

- quella degli attacchi di configurazione del sistema, mediante i quali si opera una modifica delle impostazioni sul terminale dell'utente, determinando una compromissione dei dati, come avviene quando vengono modificati i server DNS dell'utente, trasferendo la sua navigazione sul *web* verso altri siti a carattere fraudolento[112];

- quella dei *kwylogger*, ovvero dei programmi autoinstallanti sia nel *browser web* che nel *driver* del dispositivo di *input*, al fine di osservare i dati inseriti e

---

[111] FIORIGLIO G., *Sorveglianza e controllo nella società dell’informazione. il possibile contributo dell’etica hacker*, in *Nomos. Le attualità del diritto. Quadrimestrale di teoria generale, diritto pubblico comparato e storia costituzionale* 2, 2014.

[112] G. D’AIUTO, L. LEVITA, *I reati informatici. Disciplina sostanziale e questioni processuali*, cit., p. 70.

trasmettere ad un *server* di *phishing* quelli che interessano. Essi possono essere implementati tramite l'utilizzo id vari strumenti, tra cui un oggetto di *help* del *browser* che rileva le modifiche delle URL e registra le informazioni quando esso si riferisce ad un sito designato per la raccolta di credenziali, un *driver* di dispositivo che controlla l'immissione dei dati da tastiera e da *mouse* e al tempo stesso controlla le attività dell'utente. I *keylogger* possono raccogliere le credenziali relative ad un'ampia categoria di siti e spesso vengono realizzati al fine di monitorare la posizione dell'utente e trasmettere soltanto le credenziali relative a particolari siti[113].

Altra tipologia di *phishing attack* è quella realizzata mediante i motori di ricerca, ovvero attraverso la creazione di pagine *web* dedicate a prodotti fittizi, le quali sono poi indicizzate sui motori di ricerca in modo tale che gli utenti, effettuando un ordine o un'iscrizione o un trasferimento di somme, inseriscono le loro informazioni e i loro dati divenendo, in tal modo, di dominio del *phisher*[114].

Le pagine in questione offrono dei prodotti ad un prezzo molto vantaggioso; in particolare, sono state utilizzati con successo dei siti *web* di banche fraudolente. In tal modo, l'attaccante crea una *reclame* per un conto corrente, con un tasso di interesse leggermente più elevato di qualsiasi altra banca non fittizia. Gli utenti vittime trovano la banca tramite i motori di ricerca ed immettono le credenziali del loro conto bancario per un trasferimento di somme di denaro verso il nuovo

---

[113] FIORIGLIO G., *Sorveglianza e controllo nella società dell'informazione. il possibile contributo dell'etica hacker*, in *Nomos. Le attualità del diritto. Quadrimestrale di teoria generale, diritto pubblico comparato e storia costituzionale* 2, 2014.

[114] G. D'AIUTO, L. LEVITA, *I reati informatici. Disciplina sostanziale e questioni processuali*, cit., p. 78 s.

conto[115].

Il *phishing* "*man in the middle"* è una tipologia di attacco con la quale il *phisher* si interpone tra l'utente e il sito legittimo: i messaggi che sono destinati al sito legittimo passano per il tramite del *phisher*, il quale salva tutte le informazioni e i dati che possono essere di suo interesse, inoltrandoli al sito legittimo ed inviando poi all'utente le risposte di ritorno.

Tale tipologia di attacco può essere utilizzata anche per dirottare le sessioni con o senza la memorizzazione delle credenziali compromesse dell'utente.

Gli attacchi *man in the middle* sono difficili da scoprire da parte dell'utente, in quanto all'apparenza il sito funziona correttamente e potrebbe anche non esserci alcuna indicazione esterna foriera di sospetti.

Solitamente, il traffico *Secure Socket Layer* (c.d. SSL) in rete non è vulnerabile a tale tipologia di *phishing attack*, in quanto il traffico viene criptato utilizzando la chiave di sessione in modo che non possa essere decodificato da un intercettatore[116].

Tuttavia, un attacco basato sull'utilizzo di un *malware* può essere in grado di cambiare la configurazione di un sistema al fine di installare una nuova autorità di certificazione fidata e, in tal caso, un *man in the middle* può creare i propri certificati per un sito protetto con SSL, decriptare il traffico, estrarre le informazioni riservate e poi criptare nuovamente il traffico per comunicare con

---

[115] CAJANI F., COSTABILE G., MAZZARACO G., *Phishing e furto di identità digitale. Indagini informatiche e sicurezza bancaria,* cit., p. 30.

[116] G. D'AIUTO, L. LEVITA, *I reati informatici. Disciplina sostanziale e questioni processuali*, cit., p. 80 s.

l'altra parte[117].

Da ultimo, il *Rock Phish Kit* è un *software* rinvenibile *online* il quale permette la creazione di siti-clone, aventi un aspetto ed una grafica analoghi a quelli ufficiali, ma che all'interno contengono una serie di *form* da compilare per il tramite dei quali vengono captati dati sensibili alle vittime.

Tale tipologia di attacco fa utilizzo di un insieme di *software* per creare non soltanto un elevato numero di siti-clone, bensì anche un indirizzo *e-mail* da utilizzare per lo *spamming*, all'interno delle quali viene posto un *link* che reindirizza verso il sito-clone, sullo stesso *server*, in modo tale da attaccare più obiettivi diversi nello stesso momento.

Pertanto, l'attacco in questione consenta la trasformazione di ogni *server* in una base dalla quale fa partire attacchi diversi e multipli, per massimizzare le possibilità di riuscita prima che le forze dell'ordine ed i gruppi *antiphishing* riescano a neutralizzare l'attacco[118].

In buona sostanza, il *phisher* installa un pacchetto multiplo contenente i siti-clone di istituti finanziari italiani o stranieri, clonando i loghi, i testi, la grafica, trasformando il *server* ospite in una "base pronta a sferrare l'attacco" a trarre in inganno gli utenti[119].

---

[117] CAJANI F., COSTABILE G., MAZZARACO G., *Phishing e furto di identità digitale. Indagini informatiche e sicurezza bancaria,* cit., p. 29.

[118] G. D'AIUTO, L. LEVITA, *I reati informatici. Disciplina sostanziale e questioni processuali*, cit., p. 90.

[119] CAJANI F., COSTABILE G., MAZZARACO G., *Phishing e furto di identità digitale. Indagini informatiche e sicurezza bancaria,* cit., p. 30.

2.3.1 Attacchi informatici di ingegneria sociale: dalla raccolta del dato al suo impiego

Gli attaccanti iniziano il loro piano identificando il loro bersaglio, che potrebbe essere un individuo, un'azienda o persino un'istituzione governativa. Questa identificazione può avvenire attraverso una serie di metodi, tra cui ricerche online approfondite, l'analisi dei profili social media, o la semplice acquisizione di informazioni da fonti pubbliche come registri aziendali o siti web. Una volta individuato il bersaglio, gli attaccanti cercano di raccogliere informazioni altamente personalizzate. Queste informazioni possono riguardare nomi, indirizzi, date di nascita, relazioni personali, hobby e altro ancora. Questi dettagli saranno fondamentali per creare un'illusione di familiarità o credibilità quando si stabilirà il contatto con la vittima.

Successivamente, gli attaccanti passano alla fase di creazione di un pretesto. Qui, costruiscono un personaggio o un'identità falsa che sembra del tutto legittima. Possono creare account social falsi o utilizzare email e siti web contraffatti per dare credibilità al loro personaggio. Inoltre, elaborano una storia credibile o un pretesto per contattare la vittima. Questa storia può variare notevolmente, dalle richieste di assistenza tecnica apparentemente innocue alla promessa di premi immaginari o minacce fittizie[120].

Quando il pretesto è pronto, gli attaccanti passano alla fase di contatto con la vittima. Questo è il momento in cui inviano email, messaggi di testo, effettuano

[120] FIORIGLIO G., *Sorveglianza e controllo nella società dell'informazione. il possibile contributo dell'etica hacker*, in *Nomos. Le attualità del diritto. Quadrimestrale di teoria generale, diritto pubblico comparato e storia costituzionale* 2, 2014.

chiamate telefoniche o utilizzano i social media per raggiungere la vittima. Utilizzando il personaggio e le informazioni raccolte in precedenza, cercano di creare un'apparenza di autenticità per convincere la vittima a fare ciò che vogliono. Questo può includere il persuadere la vittima a condividere informazioni sensibili come password, numeri di carte di credito o addirittura l'accesso ai loro sistemi informatici[121].

Infine, quando gli attaccanti hanno ottenuto ciò che cercavano, passano alla fase di utilizzo delle informazioni ottenute. Possono utilizzare queste informazioni per accedere in modo illegittimo ai sistemi, rubare dati, installare malware o effettuare altre azioni dannose. In alcuni casi, possono anche ricattare la vittima, minacciando di rivelare le informazioni sensibili o danneggiare la loro reputazione[122].

La prevenzione degli attacchi basati sull'ingegneria sociale richiede una buona dose di consapevolezza e vigilanza. È fondamentale proteggere le informazioni personali online, utilizzare misure di sicurezza come l'autenticazione a due fattori e ricevere formazione sulla sicurezza informatica per essere in grado di riconoscere e prevenire questi tipi di attacchi. L'ingegneria sociale è un'arte subdola, ma conoscendola e difendendosi da essa, è possibile ridurre notevolmente i rischi associati.

---

[121] FIORIGLIO G., *Sorveglianza e controllo nella società dell'informazione. il possibile contributo dell'etica hacker*, in *Nomos. Le attualità del diritto. Quadrimestrale di teoria generale, diritto pubblico comparato e storia costituzionale* 2, 2014.

[122] FIORIGLIO G., *Sorveglianza e controllo nella società dell'informazione. il possibile contributo dell'etica hacker*, in *Nomos. Le attualità del diritto. Quadrimestrale di teoria generale, diritto pubblico comparato e storia costituzionale* 2, 2014.

2.4 L'evoluzione delle tecniche di attacco

Con l'evoluzione delle tecnologie, si sono evolute anche le tecniche di *phishing attack*.

Difatti, rappresenta un'evoluzione alquanto pericolosa del *phishing* il *pharming* (composto dalle parole *phishing* e *farming*): esso rappresenta una tecnica di attacco multiplo di utenti, finalizzata ad accedere a dati ed informazioni personali e riservati, senza la necessità per l'utente di aprire alcuna *e-mail*.

In buona sostanza, si tratta di una specie di truffa *on-line* consistente nella manipolazione degli indirizzi *Domain Name Server* (DNS) utilizzati dall'utente, in modo tale che le pagine *web* utilizzate dall'utente, create appositamente dagli *hacker*, non siano quelle originali, sebbene il loro aspetto e la loro grafica siano identici[123].

Al fine di comprendere meglio il fenomeno del *pharmig,* occorre precisare il concetto di manipolazione degli indirizzi DNS. Quando viene inserito un determinato indirizzo di una pagina *web* nel proprio browser in forma alfanumerica, lo stesso viene tradotto in via automatica in un indirizzo IP numerico che serve per raggiungere sul *web* il *server* corrispondente a quel dominio, poiché sarebbe troppo complesso dover ricordare sequenze di numeri che identificano tutte le pagine *web* da visitare[124].

---

[123] FIORIGLIO G., *Sorveglianza e controllo nella società dell'informazione. il possibile contributo dell'etica hacker*, in *Nomos. Le attualità del diritto. Quadrimestrale di teoria generale, diritto pubblico comparato e storia costituzionale* 2, 2014.

[124] G. D'AIUTO, L. LEVITA, *I reati informatici. Disciplina sostanziale e questioni processuali*, cit., p. 92.

La tecnica del *pharming*, attaccando i server DNS, è finalizzata a cambiare la corrispondenza numerica di tali *server,* in modo tale che essi decodifichino una corrispondenza numerica distinta da quella reale e portino l'utente ad una pagina identica a quella di riferimento, ma creata dai pirati informatici.

A questo punto, l'utente sarà convinto di navigare sul sito corretto e, nel momento in cui fa utilizzo delle proprie credenziali di accesso, le stesse, in via automatica, sono conosciute anche dal *phisher*.

Un'altra tipologia di *pharming*, più pericolosa e produttiva di effetti, è quella che si realizza a livello locale, vale a dire su ogni terminale: occorre modificare una cartella denominata "HOSTS" contenuta in ogni *computer* che faccia utilizzo di Windows quale sistema operativo ed Internet Explorer per la navigazione sul *web*, poiché nell'archivio "HOSTS" viene immagazzinata una piccola tabella con gli indirizzi di *server* ed IP più utilizzati dall'utente e, modificandola, accadrà che, nel momento in cui verrà iscritta la URL nel motore di ricerca, si verrà indirizzati in via automatica alla pagina *web* fittizia[125].

L'attaccante può far accesso nel *computer* della vittima in forma remota, oppure sfruttando qualche vulnerabilità del sistema, o mediante un *virus*

In via generale, un *pharming attack* tende ad infettare i *router* casalinghi, utilizzati per la connessione all'ADSL, i quali solitamente sono poco protetti.

La maggiore pericolosità di tale tipologia di attacchi sta nel fatto che non occorre spingere l'utente a visitare siti *fake*[126], né l'invio di *e-mail* ingannevoli: difatti, la

---

[125] G. D'AIUTO, L. LEVITA, *I reati informatici. Disciplina sostanziale e questioni processuali*, cit., p. 94.

[126] Fake significa falso.

vittima non crede di essere connessa ad un *server* trappola, in quanto questo è perfettamente simile a quello originario. Inoltre, l'evidenza dell'attacco può essere rimossa con facilità e, pertanto, la rilevanza delle attività di indagine è molto ridotta.

Vi è da dire che il fenomeno del *pharming* è in crescita, soprattutto grazie all'aumento della presenza di *malware*[127]: difatti, sempre più spesso dei programmi che appaiono innocui nascondono al loro interno dei *malware* in grado di modificare le componenti del sistema operativo, attivando dei servizi all'insaputa dell'utente.

Si prevede, inoltre, che il fenomeno sia destinato ad una forte crescita nei prossimi tempi, anche in ragione dell'incremento degli attacchi con le tecniche di *rootkit*[128], con riguardo ai quali spesso i sistemi *antimalware* si trovano in difficoltà.

Nel nostro Paese, attacchi del genere si sono verificati nell'ottobre del 2006 ad opera di un *provider* russo, con riguardo ad un indirizzo che apriva una pagina simile a quella del sito di Poste Italiane, con richiesta di inserimento di *user name* e *password* e, successivamente, l'inserimento delle 10 cifre del codice dispositivo.

La complessità di tale attacco stava nel fatto che l'indirizzo del sito era visibile

---

[127] Malware o "software malevolo" è un termine generico che descrive un programma/codice dannoso che mette a rischio un sistema.

[128] Il *Rootkit* è una tipologia di *malware* utilizzata per attaccare i *computer* ed eludere i sistemi di sicurezza, studiato in modo tale da non essere rilevato dalle applicazioni *anti-malware* e dai principali strumenti di controllo e sicurezza; esso consente all'*hacker* di installare una serie di strumenti che gli danno accesso al computer da remoto in modo che egli possa rubare *password*, informazioni bancarie e dati di carte di credito.

soltanto dai *computer* infettati da specifici *malware* e non rintracciabile con i tradizionali metodi di analisi.

Una nuova frontiera del *phishing* è lo *"Smishing",* ovvero il *phishing* attuato via SMS o di applicazioni c.d. "malevole" sugli *smartphone*, mediante i quali gli attaccanti si impossessano dei dati e delle informazioni degli utenti[129].

A questi viene inviato un messaggio sul proprio telefono portatile, soprattutto da una fonte affidabile, con l'invito a fare *click* su un *link* e la promessa di un premio o comunque una proposta particolarmente vantaggiosa e, una volta cliccato, si apre un sito creato appositamente, nel quale l'utente dovrà inserire le proprie credenziali che verranno incamerate anche dal *phisher.*

Tale tecnica si è diffusa in occasione del dilagare dei servizi automatizzati che consentono l'invio di una moltitudine di messaggi SMS in una sola volta. Difatti, gli attaccanti inviano messaggi, facendo figurare che il mittente sia un soggetto affidabile, come la banca di cui la vittima è correntista, che di solito seguono uno stesso modello, vale a dire avvisano le vittime in merito alla sussistenza di un urgente bisogno da soddisfare o della necessità di mettersi subito in contatto con il soggetto di riferimento. Qualora la vittima chiami il numero indicato nel messaggio, una voce registrata chiederà i dettagli della carta di credito e del relativo codice PIN, oltre ad altri dati e informazioni di carattere sensibile: pertanto, il *phisher* ha ottenuto ciò per cui ha posto in essere l'attacco[130].

Con il passare del tempo, la tecnica del *Smishing* si è evoluta e sempre più

---

[129] FIORIGLIO G., *Sorveglianza e controllo nella società dell'informazione. il possibile contributo dell'etica hacker*, in *Nomos. Le attualità del diritto. Quadrimestrale di teoria generale, diritto pubblico comparato e storia costituzionale* 2, 2014.

[130] V. Contraffatto, *Reati informatici*, Vicalvi, 2017, p. 19 ss.

spesso il contenuto degli SMS fraudolenti ricevuti dagli utenti non hanno più ad oggetto la richiesta di effettuare una chiamata verso un numero di telefono specifico*,* bensì di aggiornare i propri *account,* promettendo in cambio delle ricariche premio, oppure di visionare dei siti *web* commerciali e di istituti di credito, chiedendo pertanto l'inserimento delle credenziali tramite *internet.*

Tale tipologia di *phishing attack* risulta essere particolarmente pericolosa, poiché si basa sull'affidamento che gli utenti ripongono nei messaggi ricevuti da un mittente che sembra apparentemente conosciuto ed aventi un contenuto che sembra, sempre apparentemente, avere un carattere urgente[131].

Tuttavia, vi è da dire che non sempre gli attacchi in questione vengono sferrati mediante meccanismi sofisticati: difatti, di frequente il numero da comporre non riesce a gestire più di una chiamata alla volta oppure la chiamata presenta una scarsa qualità.

Al fine di tutelarsi da tali attacchi, sarebbe opportuno, una volta ricevuto l'SMS, chiedere riscontro al proprio istituto di credito o al soggetto che figura quale mittente, al fine di accertare l'effettiva autenticità del messaggio ricevuto[132].

Sempre in merito alle nuove tecniche di *phishing attack*, occorre far menzione del metodo "*Fast Flux"*: si tratta di un attacco che consente la modifica continua, a brevi lassi temporali, degli indirizzi IP e dei *domain server* dei computer attaccati dai *virus,* utilizzati al fine di ospitare dei siti di *phishing.*

Ultimamente, si sta assistendo ad un notevole aumento dei domini *Fast Flux* da

---

[131] FIORIGLIO G., *Sorveglianza e controllo nella società dell'informazione. il possibile contributo dell'etica hacker*, in *Nomos. Le attualità del diritto. Quadrimestrale di teoria generale, diritto pubblico comparato e storia costituzionale* 2, 2014.

[132] V. Contraffatto, *Reati informatici*, cit., p. 65 s.

parte dei *phisher*, poiché rendono alquanto difficoltosa l'identificazione dei siti-clone e, pertanto, risulta più complessa la loro chiusura[133].

Nei casi in questione, il moto di attacco del *phisher* muta: difatti, si assiste all'invio di una *e-mail* nella quale è presente un *link* di rimando al sito-clone dell'utente il quale, ritenendo che il messaggio si originale, clicca sullo stesso che appartiene alla rete di *pc* infettati da *malware* rispondenti ai comandi da remoto del *phisher*, inserendo le proprie credenziali sul sito-clone[134], il quale capta le credenziali e reindirizza l'utente sul sito autentico, in modo tale che egli non possa sospettare nulla[135].

Nei casi in questione, l'indirizzo IP al quale potrebbe connettersi il *browser* dell'utente muta *random* ogni pochi minuti, effettuando il collegamento a diversi *computer* che appartengono alla rete di quelli infettati da *malware* e controllati dal *phisher*: in tal modo, mediante tale cambiamento costante, diviene poco agevole risalire al *server* principale che ospita il sito clone, ed è anche più facile per il *phisher* disporre di terminali c.d. "*zombies*"[136] pronti per essere utilizzati.

Attualmente, vi sono due tipologie di rete *Fast Flux*:

- *Singol Flux;*
- *Double Flux*, la quale sfrutta una complessa tecnica basata su di un doppio livello di cambiamento degli indirizzi IP.

---

[133] FIORIGLIO G., *Sorveglianza e controllo nella società dell'informazione. il possibile contributo dell'etica hacker*, in *Nomos. Le attualità del diritto. Quadrimestrale di teoria generale, diritto pubblico comparato e storia costituzionale* 2, 2014.

[134]Tecnica c.d *back-end.*

[135] V. Contraffatto, *Reati informatici*, cit., p. 81 s.

[136]Si tratta di *computers* infettati da un *maleware* in attesa di essere attivato.

Recentemente, le aziende che producono *software antivirus* hanno scovato una particolare specie di *virus* – il *virus storm worm* – che rappresenta il principale strumento di diffusione dei *phishing attack*, la cui massima diffusione è stata registrata attraverso alcuni video caricati su YouTube[137].

Quale esempio di *Fast Flux* si può prendere in considerazione un attacco realizzato ai danni dei clienti della società Poste Italiane i quali, digitando l'URL del relativo sito *web*, di cui era stato creato un sito-clone da parte del *phisher*, hanno attivato senza volerlo un *javascript* nascosto che ha scaricato in via automatica, sul loro *pc,* un *trojan* facendo in modo che l'attaccante potesse avere accesso al *computer* del cliente.

Sebbene i responsabili della *cyber security* abbiano effettuati delle indagini finalizzate ad individuare delle strategie adeguate all'identificazione degli indirizzi IP dei siti-clone e ad effettuarne la chiusura, il *Fast Flux* rimane comunque una tecnica di attacco ad alta pericolosità, poiché è alquanto difficile individuare velocemente il sito-clone e a procedere alla sua chiusura, il quale spesso viene occultato attraverso dei *proxy*[138].

Un'altra tipologia di *phishing* è il *"Tabnabbing"* - termine che, tradotto, significa "catturare la scheda di *browser"* - ovvero una tecnica che consente di sfruttare le abitudini degli utenti di aprire più finestre (c.d. *tabs*) all'interno del *browser* durante la normale navigazione *web*, per poi consultarne una alla volta. Difatti, tramite

---

[137] FIORIGLIO G., *Sorveglianza e controllo nella società dell'informazione. il possibile contributo dell'etica hacker*, in *Nomos. Le attualità del diritto. Quadrimestrale di teoria generale, diritto pubblico comparato e storia costituzionale* 2, 2014.

[138] CAJANI F., COSTABILE G., MAZZARACO G., *Phishing e furto di identità digitale. Indagini informatiche e sicurezza bancaria,* cit., p. 41.

tale tecnica, l'utente del *web*, navigando sulla rete, apre una pagina apparentemente innocua, la quale non richiede l'inserimento di *password* o altri dati ma che, al contrario, presenta un contenuto di interesse, spesso immagini *hot* e, pertanto, l'utente non la chiude, passando a visionare un'altra finestra del *browser*.

Ciò che accade è che la scheda-trappola, mentre l'utente continua a navigare sul *web*, si trasforma e cambia la propria icona[139] e il proprio contenuto, divenendo la pagina che richiede di autenticarsi per utilizzare un servizio adoperato dall'utente. Si pensi, ai fini esemplificativi, alla pagina di accesso alla propria banca, alla propria casella di posta, al proprio *account social.*

In tal modo l'utente, vedendo l'icona del sito conosciuto sulla pagina *web,* pensa di essere stato lui ad aprirla e procede ad inserire le proprie credenziali di accesso senza controllare che l'URL della pagina sia effettivamente corretto[140].

A questo punto, il *phisher* entra in possesso delle credenziali di autenticazione della vittima tramite lo *script* fraudolento che procede a memorizzarle, trasmigrando poi l'utente – il quale ignora di essere stato derubato del proprio *account* – sulla vera pagina, autenticandolo sul sito.

Al fine di tutelarsi contro tale tipologia di *phishing attack* è opportuno aprire una scheda nuova per fare il *login* in qualunque servizio, scrivendo manualmente l'indirizzo della pagina oppure inserendolo tra i Preferiti, soprattutto nel caso in cui viene chiesto di inserire le proprie credenziali di autenticazione[141].

---

[139]Ciò viene detto "*Favicon"*.

[140] V. Contraffatto, *Reati informatici*, cit., p. 90.

[141] D'AIUTO G., LEVITA L., *I reati informatici. Disciplina sostanziale e questioni processuali*, Milano, 2012, p. 55 ss.

Infine, altra tecnica altamente diffusa è quella del *vishing* – termine che rappresenta una fusione tra le parole *"Voice over Internet Protocol* e *phishing* – la quale si sostanzia nell'invio da parte del c.d. *visher* di una *e-mail* che appare identica, nella grafica e nel contenuto, a quella di una società o un ente conosciuto dal destinatario, come la sua banca o un sito al quale la vittima è veramente iscritto, contenente degli avvisi relativi a problemi che si sono verificati sul proprio conto corrente o *account*, come un addebito economico o l'avvenuta scadenza dell'*account,* invitando il destinatario a comporre un numero telefonico per evitare l'addebito della somma o a regolarizzare la sua posizione con l'ente o la società.

La vittima, una volta composto il numero di telefono, prenderà contatto con un finto *call-center* il quale chiederà di fornire i propri dati personali, come il numero di conto corrente o della carta di credito: in tal modo, le informazioni raccolte saranno utilizzate dal *visher* per effettuare degli acquisti, trasferire delle somme di denaro o anche soltanto per effettuare degli attacchi ulteriori, magari facendo utilizzo dell'identità di un altro individuo[142].

Altra tecnica di *vishing* è quella consistente nell'attivare un *account Voice over Internet Protocol* (VoIP) e nell'avvio di un sistema di chiamata automatico al fine di prendere contatti con le potenziali vittime, invitandole, mediante la riproduzione di una registrazione vocale, a comporre un numero di telefono, il quale viene spacciato per un *call center* in grado di risolvere delle problematiche o fornire

[142] SURACE C., *Dal Phishing al Vishing*: *l'evoluzione della truffa come conseguenza dell'evoluzione tecnologica,* (a cura di), Ricerca svolta presso l'Osservatorio CSIG (Centro Studi Informatica Giuridica) di Reggio Calabria, in www.filodiritto.com, 2007.

comunicazioni urgenti sul proprio conto corrente o sulla propria carta di credito, previo inserimento dei propri dati personali, ma in realtà si tratta del numero VoIP del *visher*[143].

Invero, corre l'obbligo di evidenziare come il fenomeno dei falsi *call center* sia ormai in costante crescita: gli attaccanti fanno leva sulla circostanza che vi è meno differenza a comunicare i propri dati personali a voce, ad un soggetto che lavora per un *call center* e non rispondere ad una semplice *e-mail*[144].

Vi è da dire che il ruolo dei *financial manager* risulta strettamente collegato al fenomeno del *vishing*: si tratta di soggetti che pongono a disposizione i propri conti correnti per il deposito di somme di denaro sottratte dai *phisher* alle vittime mediante le tecniche già descritte e, una volta che le somme sono state accreditate, le prelevano e le trasferiscono all'estero dietro compenso.

Invero, i *phisher* hanno necessità di essere affiancati da un *financial manager*, in quanto, dopo aver acquisito le credenziali e la possibilità di effettuare dei fraudolenti bonifici *on-line*, debbono incassare le relative somme, poiché il sistema di *home-banking* italiano non consente di effettuare dei bonifici verso Paesi esteri senza essere sottoposti al controllo degli istituti bancari[145].

Pertanto, accade spesso che, in concomitanza all'invio delle *e-mail* di *phishing*, viene registrata la richiesta di collaborazione, spesso inviata tramite messi di

---

[143] D'AIUTO G., LEVITA L., *I reati informatici. Disciplina sostanziale e questioni processuali*, Milano, 2012, p. 61 ss.

[144] SAMBUCCI L., *Falsi call center sul VoIP: la nuova truffa si chiama Vishing,* in *www.anti-phishing.it* , 2006.

[145] D'AIUTO G., LEVITA L., *I reati informatici. Disciplina sostanziale e questioni processuali*, Milano, 2012, p. 71 ss.

posta elettronica che provengono da finte società estere, indirizzata a cittadini italiani o che risiedono in Italia.

A questi soggetti verrà chiesto di comunicare le coordinate del proprio conto corrente, in quanto l'attività che verrà loro proposta consisterà nel prelievo di somme di denaro che vengono accreditate di volta in volta su tali conti e che provengono in apparenza da clienti di tali società ma che, in realtà, provengono dai soggetti truffati, al fine di ritrasferirle all'estero[146].

In questo caso, il reato che viene in questione è il riciclaggio di denaro: il *financial manager* trasferisce delle risorse che provengono da un'attività illecita da parte di un soggetto estraneo alla commissione del reato presupposto, così come viene previsto e punito dal reato di riciclaggio, di cui all'art. 648 *bis*, c.p.

2.5 Gli effetti e le conseguenze del phishing sulle vittime e sulle organizzazioni colpite

Gli effetti del phishing sono assai significativi, variando a seconda della vittima di riferimento. Anzitutto, rappresenta una minaccia diretta per le finanze delle vittime. Gli attaccanti utilizzano inganni sofisticati per ottenere informazioni finanziarie sensibili, come i numeri delle carte di credito e le password di accesso ai conti bancari. Una volta in possesso di queste informazioni, possono compiere transazioni non autorizzate direttamente dai conti delle vittime[147]. Questo si

[146] CAJANI F., *Profili penali del phishing*, in *C.P.,* 2007, p. 2294.

[147] D'AIUTO G., LEVITA L., *I reati informatici. Disciplina sostanziale e questioni processuali*, Milano, 2012, p. 80 s.

traduce in un danno finanziario immediato e tangibile per le vittime. Ad esempio, possono scoprire addebiti non autorizzati sui loro conti o ricevere estratti conto che mostrano transazioni non riconosciute[148].

Inoltre, spesso le vittime non si accorgono immediatamente delle transazioni fraudolente, il che consente agli attaccanti di accumulare ulteriori danni finanziari prima che la frode venga scoperta. Affrontare il furto di denaro richiede tempo e sforzi, poiché le vittime devono contestare le transazioni e richiedere il rimborso. Tuttavia, il recupero completo dei fondi rubati non è garantito, e ciò può comportare costi accessori, come tasse bancarie o spese legali, per ripristinare i propri conti finanziari.

Oltre al furto diretto di denaro, il phishing può condurre a frodi finanziarie più complesse. Gli attaccanti possono utilizzare le informazioni finanziarie rubate per condurre attività dannose a lungo termine, come l'apertura di nuovi account finanziari a nome delle vittime. Questi account possono essere utilizzati per ulteriori frodi, come richiedere carte di credito supplementari o accumulare debiti che le vittime sono obbligate a ripagare.

Una conseguenza particolarmente dannosa è rappresentata dai prestiti fraudolenti. I truffatori possono richiedere prestiti o finanziamenti utilizzando le informazioni delle vittime, accumulando debiti significativi a nome delle vittime stesse. Questo non solo comporta un danno finanziario immediato, ma può anche danneggiare il credito delle vittime, rendendo difficile ottenere prestiti futuri o richiedere credito[149].

---

[148] V. Contraffatto, *Reati informatici*, cit., p. 101.

[149] V. Contraffatto, *Reati informatici*, cit., p. 105.

Le organizzazioni sono anch'esse suscettibili di essere vittime di attacchi di phishing. Quando ciò accade, possono verificarsi gravi conseguenze legate alla divulgazione di informazioni aziendali sensibili:

- **Rischio per i segreti commerciali:** Gli attaccanti possono ottenere accesso a dati sensibili delle aziende, come segreti commerciali, progetti in corso, piani strategici o proprietà intellettuale. Queste informazioni possono essere utilizzate per ottenere un vantaggio competitivo o vendute a concorrenti o criminali.
- **Violazione della privacy dei clienti:** Se le informazioni dei clienti vengono compromesse, le organizzazioni possono affrontare gravi conseguenze legali e finanziarie. La divulgazione non autorizzata di dati dei clienti può comportare denunce, multe e danneggiare irrimediabilmente la reputazione dell'azienda[150].
- **Perdita di fiducia dei clienti:** Le violazioni della sicurezza dei dati possono erodere la fiducia dei clienti nell'azienda. I clienti potrebbero essere riluttanti a condividere ulteriori informazioni personali o finanziarie con l'azienda, causando un impatto duraturo sulla base clienti e sulle entrate[151].

L'aspetto della perdita di fiducia e del danno di immagine non è da sottovalutare. Quando organizzazioni come banche, istituti finanziari o enti governativi sono coinvolte in casi di phishing, si verificano effetti a cascata sulla percezione del

[150] C. Sarzana di S. Ippolito, *Informatica, internet e diritto penale*, Milano, 2010, p. 16 ss.
[151] D'AIUTO G., LEVITA L., *I reati informatici. Disciplina sostanziale e questioni processuali*, Milano, 2012, p. 90.

pubblico di queste istituzioni. Il coinvolgimento di queste istituzioni in casi di phishing può far percepire al pubblico una mancanza di sicurezza informatica efficace. I clienti e i cittadini potrebbero dubitare della capacità di queste organizzazioni di proteggere in modo adeguato le informazioni sensibili. La fiducia è un elemento chiave per la stabilità e il funzionamento delle istituzioni. Quando il pubblico perde fiducia in banche, istituzioni finanziarie o enti governativi, possono sorgere problemi di instabilità finanziaria o di governabilità[152].

La perdita di fiducia può portare anche a una reputazione danneggiata per queste istituzioni. Anche se la violazione di sicurezza è il risultato di un attacco esterno, l'associazione con un caso di phishing può causare un danno significativo alla reputazione.

Le aziende che diventano vittime di attacchi di phishing possono subire gravi conseguenze a livello di immagine e reputazione: le notizie su violazioni della sicurezza e attacchi di phishing possono diffondersi rapidamente attraverso i media e i canali digitali. Questa esposizione pubblica negativa può danneggiare l'immagine dell'azienda e influenzare negativamente la percezione dei clienti[153].

La pubblicità negativa e la preoccupazione per la sicurezza possono portare alla perdita di clienti esistenti. I clienti possono decidere di interrompere le relazioni commerciali con l'azienda a causa delle preoccupazioni sulla protezione dei loro dati. Infine, l'immagine di un'azienda colpita da un attacco di phishing può

[152] C. Sarzana di S. Ippolito, *Informatica, internet e diritto penale*, cit., p. 33 ss.

[153] D'AIUTO G., LEVITA L., *I reati informatici. Disciplina sostanziale e questioni processuali*, Milano, 2012, p. 92.

scoraggiare potenziali clienti dall'acquistare i suoi prodotti o servizi. La reputazione dell'azienda può subire un danno a lungo termine che influisce sulle vendite e sulla crescita[154].

[154] C. Sarzana di S. Ippolito, *Informatica, internet e diritto penale*, cit., p. 65 ss.

CAPITOLO III
Strumenti penali di contrasto e analisi della casistica giurisprudenziale

3.1 Inquadramento del fenomeno del phishing all'interno dell'ordinamento penale

Dopo aver chiarito, dal punto di vista pratico, il phishing, pare opportuno inquadrare il fenomeno dal punto di vista giuridico. Nell'ordinamento giuridico italiano non si rinviene una normativa specifica che si occupi di definire e sanzionare il fenomeno illecito del *phishing*.

Di conseguenza, le condotte illecite riconducibili a tale fenomeno vengono ricomprese, caso per caso, a seconda della manifestazione e del *modus operandi,* nell'ambito delle diverse fattispecie civili o penali già previste dalla legge, poiché si è in presenza di un fenomeno che attualmente è in continua evoluzione[155].

A seguito delle prime manifestazioni di *phishing*, avvenute nel 2005, vi sono state due interrogazioni parlamentari[156] aventi lo scopo di porre in evidenza la necessità di incrementare gli interventi di polizia postale nonché di realizzare delle concrete iniziative per eliminare in radice tale fenomeno illecito.

In risposta a tali interrogazioni[157], la polizia postale, in collaborazione con l'Associazione Bancaria Italiana (ABI) e Poste Italiane, ha dato avvio ad un'attività di sensibilizzazione degli utenti la quale, mediante gli istituti bancari, vengono avvisati del pericolo rappresentato dal fenomeno del *phishing*.

---

[155] D'AIUTO G., LEVITA L., *I reati informatici. Disciplina sostanziale e questioni processuali*, Milano, 2012, p. 55 s.

[156]Cfr. Camera dei Deputati, Resoconto stenografico seduta n. 82 del 5 dicembre 2006, p. 2708, in *www.camera.it.*

[157]Cfr. Camera dei deputati, Resoconto stenografico seduta n. 101 del 31 gennaio 2007, p. 40, in *www.camera.it.*

Dal punto di vista della repressione di tale condotta illecita, la polizia postale ha avviato quasi 1.200 indagini di propria iniziativa nonché altre 900 su richiesta dell'autorità giudiziaria: gli interventi in questioni hanno consentito di denunciare circa 80 persone nonché di procedere a perquisizioni. Ne è derivato che la maggior parte delle minacce proveniva da Paesi dell'Europa orientale.

Poiché, come si è già anticipato, il legislatore non si è ancora occupato di dettare una disciplina specifica per i *phishing attacks*, al fine di comprendere quale delle norme attuali si possano concretamente applicare ai singoli casi di specie, occorre ben considerare ogni fase in cui l'attacco può suddividersi.

Ed invero, in tal senso si distingue una prima fase, consistente nell'invio di un messaggio *e-mail* avente ad oggetto un *link* di rinvio alla pagina *web* non autentica, finalizzato a spingere l'utente a rivelare proprie informazioni personali riservate. La seconda fase consiste nella “raccolta” dei dati riservati dell'utente attraverso tale sito oppure mediante un *form* da compilare con le informazioni personali richieste. Infine, nella terza fase vi è l'utilizzo delle informazioni raccolte al fine di accedere ai servizi *on-line* o alle aree riservate in maniera abusiva, oppure allo scopo di utilizzare in maniera indebita carte di credito o di pagamento, realizzando un profitto.

Orbene, nell'esaminare le norme penali che possono applicarsi astrattamente ai singoli casi di *phishing attack*, risulta opportuno mantenere la distinzione in fasi, sebbene nella consapevolezza che alcune ipotesi delittuose possono ricondursi a più fasi.

Con riferimento specifico alla prima fase degli attacchi in commento – relativa all'invio di messaggi di posta elettronica soltanto in apparenza provenienti da

mittenti “reali” - potrebbe prospettarsi l'applicazione della fattispecie penale di cui all'art. 494 c.p.[158], nel caso in cui vengano utilizzati *on-line* gli estremi identificativi di un reale mittente, in modo tale da configurare le modalità tassativamente previste dal reato di sostituzione di persona o della riconducibilità “*a sé o ad altri di un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici”*

Le condotte che caratterizzano tale prima fase possono in realtà essere realizzate anche nella terza fase, nella quale il *phisher* fa utilizzo dei dati raccolti, al fine di accedere ad aree o servizi *on-line* riservati, ponendo in essere attività illecite.

Qualora la condotta finalizzata alla raccolta delle credenziali viene realizzata mediante la collocazione di un *virus*, su un sito internet appositamente creato oppure in un allegato ad un messaggio *e-mail* preventivamente inviato all'utente, si può ulteriormente ritenere applicabile, nella prima fase, l'art. 615 *quinquies* c.p., che disciplina il caso di diffusione di programmi diretti a danneggiare o interrompere un sistema informatico.

Il carattere offensivo del *phishing attack* si manifesta soprattutto nella seconda fase, deputata alla “raccolta” o “pesca” dei dati personali degli utenti. In proposito, la dottrina si è domandata se la fase in questione possa ricondursi alle condotte tipiche della fattispecie di “detenzione e diffusione abusiva dei codici di accesso

[158]L'art. 494 c.p prevede espressamente che “*Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici, è punito, se il fatto non costituisce un altro delitto contro la fede pubblica, con la reclusione fino ad un anno”.*

a sistemi informatici o telematici", di cui all'art. 615 *quater* c.p.[159]., nonché se fra le modalità di realizzazione del fatto tipico possa includersi anche l'invio di un messaggio di posta elettronica avente un contenuto tale da spingere il destinatario a fornire informazioni riservate.

La norma in questione deve essere interpretata tenendo in considerazione l'elemento di illiceità speciale che caratterizza le condotte, coinvolgendo le medesime modalità fraudolente di raccolta dei codici di accesso, per cui il legislatore non ha espressamente previsto delle forme vincolate[160].

Pertanto, nulla osta ad includere nell'espressione "procurarsi abusivamente" anche l'invio di un messaggio di posta elettronica che contribuisca all'effettiva raccolta di tali credenziali di accesso. Difatti, queste ultime rappresentano l'oggetto materiale su cui ricade l'attività del soggetto agente: esse possono sostanziarsi in qualsiasi codice numero, alfabetico e alfanumerico, includendo fra gli altri "altri mezzi idonei all'accesso" anche l'indirizzo *e-mail* o il numero della propria carta di credito o di debito, qualora servano ad identificare l'utente per consentirgli di accedere ai servizi telematici, in abbinamento con *password* o parole chiave.

La "raccolta" o "pesca" dei dati riservati dell'utente – con sottrazione ed impossessamento degli stessi – hanno fatto pensare alla possibile applicazione,

---

[159]L'art. 615 *quater* c.p dispone espressamente che "*Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino ad euro 5.164".*

[160] C. Sarzana di S. Ippolito, *Informatica, internet e diritto penale*, cit., p. 78 ss.

nella seconda fase dell'attività di *phishing attack*, della fattispecie penale del furto *ex* art. 624 c.p.[161].

Tuttavia, a ben vedere, non sembrerebbe possibile applicare la norma in questione, in quanto la "raccolta" di dati riservati non rappresenta né un "impossessamento", né una "sottrazione di cosa mobile altrui". Ed invero, i dati riservati e le informazioni personali dell'utente non sono idonei ad essere "sottratti", rimanendo a disposizione anche del titolare, poiché non si verifica l'acquisizione di un potere di dominio esclusivo da parte del *phisher*.

Peraltro, le modalità secondo cui si manifestano le condotte di furto presuppongono l'usurpazione in via unilaterale nonché il dissenso del soggetto passivo, il quale non si realizza nella seconda fase del *phishing*, dato che sussiste una cooperazione della vittima che, sebbene indotta in errore tramite il contenuto dell'*e-mail* ed il sito non autentico, fornisce i propri dati riservati[162].

Alla terza fase del *phishing* – finalizzata all'utilizzo dei dati riservati raccolti – si può applicare la fattispecie penale della frode informatica, in presenza degli elementi costitutivi del reato di cui all'art. 640 *ter* c.p.[163].

---

[161]L'art. 624 c.p afferma espressamente che "*chiunque si impossessa della cosa mobile altrui, sottraendola a chi la detiene, al fine di trarne profitto per sé o per altri, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 154 a ero 516. Agli effetti della legge penale, si considera cosa mobile anche l'energia elettrica e ogni altra energia che abbia un valore economico".*

[162] C. Sarzana di S. Ippolito, *Informatica, internet e diritto penale*, cit., p. 92 ss.

[163]La norma in questione afferma che "*chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032".*

Si pensi al caso in cui il *phisher*, mediante l'utilizzo dei dati riservati raccolti, intervenga telematicamente sui dati, sulle informazioni o sui programmi dell'utente, modificando i dati relativi alle operazioni bancarie e finanziarie, oppure relative al conto corrente, al fine di procedere ad addebiti, a trasferimenti di fondi, all'utilizzo indebito di carte di credito o di pagamento o ad ogni altro abuso di simili servizi *on-line*.

Qualora invece tali operazioni venissero poste in essere mediante o a seguito di un accesso abusivo ad uno o più sistemi informatici, si potrebbe configurare un concorso formale di reati di cui all'art. 615 *ter* c.p.[164], astrattamente configurabile. Inoltre, l'utilizzo dei dati e delle informazioni è legato all'accesso abusivo ad aree informatiche riservate o a servizi *on-line* per lo svolgimento di operazioni bancarie o finanziare, pertanto è astrattamente applicabile anche il solo art. 615 *ter* c.p.

Può trovare applicazione in tale fase anche l'art. 640 c.p.[165] che disciplina la truffa, poiché il *phisher*, mediante artifici e raggiri realizzati mediante l'invio di falsi messaggi di posta elettronica e la creazione di false pagine *web* del tutto analoghi a quelli di primari istituti di credito, dopo aver indotto in errore l'utente ed aver carpito fraudolentemente le credenziali di accesso, si introduce nel servizio di *home banking* della vittima al fine di svolgere delle operazioni di prelievo o di bonifico non autorizzate.

---

[164]Così recita la norma di cui all'art. 615 *ter*: "*chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni".*

[165]E' possibile applicare la fattispecie di truffa anche alle prime due fasi dei *phishing attacks*: false *e-mail* e falsi siti *web* quali artifici e raggiri, in riferimento alla fase dell'"esca"; successivamente, l'induzione in errore e la rivelazione da parte dell'utente delle credenziali, in riferimento alla fase della "pesca".

3.1.1 Le truffe attraverso il *phishing*

Come si è detto poc'anzi, l'attività di *phishing* può ricondursi alla fattispecie di truffa di cui all'art. 640 c.p., tutte le volte in cui il *phisher,* ponendo in essere artifici e raggiri determinati dalla sostituzione di persona – realizzata mediante la creazione ed utilizzazione di un falso *account* di posta elettronica attribuibile ad un apparente vero e diverso soggetto – dopo aver indotto in errore la vittima ed essersi fatto rivelare i codici di accesso, si introduce nel suo servizio di *home-banking*, compiendo degli atti dispositivi determinanti un impoverimento del patrimonio della vittima, con pari profitto in proprio favore[166].

L'elemento oggettivo del reato si identifica con la condotta del soggetto agente, il quale induce in errore la persona offesa, millantando di essere la propria banca di fiducia o una nota società di *e-commerce,* inducendo la vittima a comunicare i propri dati riservati.

In seguito, il soggetto indotto in errore realizza l'atto di disposizione patrimoniale, il quale è causa dell'ingiusto profitto con altrui danno.

D'altronde, l'appropriazione fraudolenta di codici e *password* non è altro che lo strumento attraverso il quale il *phisher* è in grado di ottenere, mediante gli artifici e i raggiri tipici di tale fenomeno illecito, l'indebito profitto patrimoniale, realizzando in tal modo la condotta e l'evento propri della truffa[167].

A sostegno del fatto che il comportamento illecito del *phisher* può integrare lo

---

[166] V. Di Lembo, *Il "phishing": dall'illecita captazione di dati alla truffa*, in *Rassegna dell'Arma dei Carabinieri*, 4, 2013, pp. 67-71

[167]In tal senso FANELLI A., *Commento all'art. 640 c.p.,* in LATTANZI-LUPO, *Codice penale, Rassegna di giurisprudenza e di dottrina,* Milano, 2005, p. 157.

schema dell'induzione in errore del soggetto passivo – tipico *modus operandi* della fattispecie penale della truffa *ex* art. 640 c.p. – si può richiamare una nota sentenza della giurisprudenza di merito[168].

In tale pronuncia, i giudici hanno affermato la configurabilità degli artifici e dei raggiri nella condotta di colui che utilizza un messaggio di posta elettronica nel quale vengono riprodotti colori, marchi ed altre caratteristiche di organizzazioni reali.

Trattandosi di tipico reato contro il patrimonio, la truffa si caratterizza per l'inganno mediante il quale il soggetto agente induce la vittima al compimento di un atto che determina un depauperamento del proprio patrimonio il quale consiste specificamente, nel caso del *phishing*, nell'invio multiplo di false *e-mail* dal contenuto ingannevole, apparentemente provenienti da enti affidabili, le quali invitano gli utenti ignari a comunicare le proprie credenziali di accesso.

Pertanto, le ipotesi comuni di *phishing* – che si sostanziano nella captazione abusiva di dati riservati, utilizzati per il prelievo di somme di denaro – possono rientrare nell'ambito applicativo della fattispecie penale *ex* art. 640 c.p. Ed invero, nei falsi messaggi di posta elettronica si rinviene l'elemento degli artifici e dei raggiri, l'induzione in errore del cliente dell'istituto bancario nonché l'ingiusto profitto con altrui danno[169].

---

[168]Cfr. Trib. Milano, sent. 7 ottobre 2001, n. 11696, in *www.leggiditalia.it*

[169]Di tale avviso AMORE S., STANCA V., STARO S., *I crimini informatici. Dottrina, giurisprudenza ed aspetti tecnici delle investigazioni,* Massa Carrara, 2006, p. 73.

3.1.2 Profili rilevanti nelle frodi informatiche attraverso il *phishing*

Si è ritenuto che la condotta di *phishing* possa configurare anche il reato di frode informatica, previsto e punito dall'art. 640 *ter* c.p., determinando l'induzione in errore del soggetto che, inconsapevolmente, fornisce i propri dati e le proprie informazioni riservate, mediante un intervento, *sine titulo,* nel sistema informatico di un istituto bancario o di altro ente.

Ed invero, la condotta del *phisher* sembra ricondursi ad una frode compiuta con abilità mediante mezzi informatici, anche tenendo in debita considerazione i beni giuridici tutelati dalla norma richiamata, ovvero il patrimonio del danneggiato, l'interesse alla regolarità del corretto funzionamento dei sistemi informatici, nonché la riservatezza del relativo utilizzo.

Tuttavia, l'elemento oggettivo della fattispecie in questione richiede che venga necessariamente posta in essere una delle due condotte tipiche previste dalla norma, vale a dire l'alterazione del funzionamento del sistema informatico o l'intervento su dati o programmi contenuti nel sistema.

Da ciò ne deriva che, la mera acquisizione o duplicazione dei dati non è sufficiente ad integrare l'elemento materiale del reato di frode informatica, potendo invece ricondursi a tale reato soltanto quegli interventi finalizzati a determinare delle alterazioni del funzionamento del sistema o manipolazioni arbitrarie dei suoi contenuti. In tal senso, si pensi al caso dell'utilizzo della *password,* ottenuto in modo illecito, al fine di accedere al sistema informatico di *home banking* dell'utente, per poi effettuare un bonifico dal relativo conto

corrente[170]; oppure si pensi al caso in cui vengono utilizzati i c.d. programmi *key-logger*, al fine di introdursi nei *computer* degli utenti ed estrarre abusivamente dati ed informazioni sulle operazioni compiute mediante tali sistemi informatici[171]. Pertanto, nei casi di *phishing* fondati su *malware,* il ricorso ad un *software* malevolo che si auto-installa sul *computer* della vittima potrebbe integrare gli estremi del reato di frode informatica in quanto, ad ogni modo, attraverso tale condotta il *phisher* inserisce un elemento nel sistema senza il consenso tacitamente o espressamente fornito dall'utente[172].

In considerazione del fatto che l'attività di *phishing* prevede l'invio, da parte del soggetto agente, di messaggi di posta elettronica riproducenti la grafica e i loghi ufficiali di organizzazioni aziendali o istituzionali – come quelli di istituti bancari o postali – nei confronti di un elevato numero di destinatari, tale condotta può integrare pacificamente il furto o l'indebito utilizzo dell'identità digitale di uno o più soggetti, circostanza aggravante del reato di frode informatica[173].

A questo punto, appare doveroso verificare il rapporto tra l'art. 494 c.p. - secondo l'interpretazione estensiva al mondo *on-line* fornita dalla Cassazione[174] – e l'art.

---

[170]Cfr. Cass. Pen., sent. 24 febbraio 2011, n. 9891, in *www.italgiure.giustizia.it.*

[171] D'AIUTO G., LEVITA L., *I reati informatici. Disciplina sostanziale e questioni processuali*, Milano, 2012, p. 33 ss.

[172]Cfr. FLOR R., *Phishing, identify theft e identify abuse: le prospettive applicative del diritto penale vigente,* in *Riv. it. Dir. Proc. Pen.,* 2007, p. 905.

[173]La circostanza aggravante in questione è stata introdotta al terzo comma dell'art. 640 *ter* c.p., ad opera della Legge n. 93/2013.

[174]Cfr. Cass Pen., sent. 8 novembre 2007, n. 46674, in *www.leggiditalia.it,* secondo la quale "*integra il reato di sostituzione di persona, art. 494 c.p., la condotta di colui che crei ed utilizzi un account di posta elettronica, attribuendosi falsamente le generalità di un diverso soggetto, inducendo in errore gli utenti della rete internet nei confronti dei quali le false generalità siano declinate e con il fine di arrecare danno al soggetto le cui generalità siano state abusivamente*

640 *ter* c.p.

Al riguardo, la presenza, nel disposto dell'art. 494 c.p., della clausola di riserva "*se il fatto non costituisce un altro delitto contro la fede pubblica",* sembrerebbe non porre alcun problema riguardo alla possibilità di un concorso materiale tra i due reati, in considerazione dei beni e degli interessi differentemente tutelati.

Tuttavia, sebbene possa riconoscersi astrattamente una sovrapponibilità tra la condotta di colui che "*sostituisca illegittimamente la propria all'altrui persona, o attribuisca a sé o ad altri un falso nome, un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici"* e quella di chi "*rubi o indebitamente utilizzi un'identità digitale con altrui danno"*[175]*,* sembra forse più correttamente sostenibile, nella maggior parte dei casi ipotizzabili, la tesi che vede un concorso formale di reati, riconoscendo alla nuova previsione dell'art. 640 *ter*, comma 3, c.p. la natura di reato complesso.

Appare opportuno verificare anche l'applicabilità del terzo comma dell'art. 640 *ter* ad ulteriori ipotesi delittuose come, ad esempio, le truffe su piattaforme di commercio elettronico o i casi di acquisizione indebita di un *account* personale o di un profilo su una piattaforma *social*[176]*.*

Nel caso delle truffe su piattaforme di *e-commerce,* da un lato viene realizzato sia il furto di identità dell'utente tramite messaggio *e-mail* di *phishing* che sembra

---

spese, subdolamente incluso in una corrispondenza idonea a lederne l'immagine e la dignità (nella specie a seguito dell'iniziativa dell'imputato, la persona offesa si ritrovò a ricevere telefonate da uomini che le chiedevano incontri a scopo sessuale)".

[175]Cfr. FLOR R., *Phishing, identify theft e identify abuse: le prospettive applicative del diritto penale vigente,* cit., p. 908.

[176] D'AIUTO G., LEVITA L., *I reati informatici. Disciplina sostanziale e questioni processuali*, Milano, 2012, p. 45 ss.

apparentemente provenire dalla società che gestire la piattaforma di commercio elettronico e, dall'altro, una volta acquisita tale finta identità digitale, vengono effettuate delle fittizie inserzioni di vendita, aventi il fine di ottenere pagamenti anticipati tramite carte ricaricabili, le quali anch'esse sono oggetto di precedente furto di identità.

Pertanto, il nuovo disposto dell'art. 640 *ter,* comma terzo, c.p., sembrerebbe astrattamente in grado di disciplinare in maniera più adeguata tali ipotesi delittuose rispetto agli artt. 494 e 640 c.p. poiché è pacifico che, nella condotta successiva al furto di identità digitale e consistente nella realizzazione delle inserzioni di vendita fittizie, possa realizzarsi un'ipotesi di intervento senza diritto sui dati e/o sulle informazioni contenuti nel sistema informatico messo a disposizione dell'utente originario dalle richiamate società di commercio elettronico.

Parimenti è a dirsi con riguardo alle ipotesi – finora riconducibili agli artt. 494 e 615 *ter* c.p. - di acquisizione indebita di un *account* personale o di un profilo su una piattaforma *social*[177]*.*

Ed invero, anche in tali ipotesi, subito dopo la condotta di accesso abusivo al relativo sistema informatico, si configura, nella condotta finalizzata all'utilizzo, a fine di profitto e con altrui danno, della identità digitale così illecitamente acquisita, un intervento *sine titulo* su dati e/o informazioni contenuti in tale sistema informatico[178].

---

[177] D'AIUTO G., LEVITA L., *I reati informatici. Disciplina sostanziale e questioni processuali*, Milano, 2012, p. 50 ss.

[178] V. Di Lembo, *Il "phishing": dall'illecita captazione di dati alla truffa*, cit., p. 69.

Un altro elemento di favore per la configurabilità del reato di frode informatica nel caso di attività di *phishing* è l'evento di tale fattispecie di reato, consistente nel conseguimento, da parte del soggetto attivo, di un ingiusto profitto con altrui danno, avente carattere economico-patrimoniale[179]. In caso di *phishing,* il profilo economico perseguito dall'*hacker* integra tale astratta determinazione di impoverimento patrimoniale cui corrisponde l'ingiusto arricchimento del reo.

3.1.3 Analisi tecnica dell'accesso abusivo ad un sistema informatico o telematico

L'accesso abusivo nell'*account* di un soggetto, in elusione delle misure di autenticazione e identificazione predisposte al fine di garantire la tutela dei dati in esso contenuti, ovvero l'esatta condotta del *phisher*, può integrare il reato di "*accesso abusivo ad un sistema informatico o telematico"*, disciplinato dall'art. 615 *ter* c.p.

Il reato in questione si perfeziona con l'introduzione in un sistema rappresentato da un insieme di strumenti che fanno utilizzo di tecnologie informatiche, come nel caso in cui il *phisher* effettua l'accesso al servizio di banca digitale della vittima, a seguito dell'illecita captazione dei suoi codici di accesso[180].

Ed invero, l'intrusione abusiva o la permanenza indebita nei sistemi informatici, contro la volontà dell'avente diritto – persona fisica o giuridica – determina una compromissione dell'interesse tutelato dalla norma, vale a dire la riservatezza del domicilio informatico, da intendere quale "*luogo in cui può estrinsecarsi la*

[179]Cfr. Cass Pen., sent. 24 novembre 2003, n. 4576, in *Giur. It.,* 2004, p. 2363.

[180] V. Di Lembo, *Il "phishing": dall'illecita captazione di dati alla truffa*, cit., p. 70.

personalità individuale", che rappresenta la trasposizione sul piano virtuale dello *jus excludendi alios*, ovvero il diritto del titolare di impedire ad altri l'accesso indesiderato allo spazio informatico di sua pertinenza, protetto da misure di sicurezza[181].

Il delitto di cui all'art. 615 *ter* c.p. si configura anche a carico di chi, sebbene autorizzato ad accedere ad un sistema informatico per alcune finalità, utilizzi tale facoltà per finalità diverse rispetto a quelle per le quali l'autorizzazione era stata concessa.

Pertanto, l'art. 615 *ter* c.p. sanziona penalmente non soltanto colui che si inserisce abusivamente in un sistema informatico o telematico protetto da misure di sicurezza – introduzione abusiva non configurabile in capo al soggetto autorizzato all'accesso al sistema e che, pertanto, è munito dei codici necessari per superare le misure di sicurezza senza violarle – ma anche il soggetto che, dopo essersi introdotto lecitamente nel sistema informatico, vi si mantiene contro la volontà espressa o tacita di colui che ha il diritto di escluderlo, come previsto dalla seconda parte del primo comma[182].

Difatti, colui che sfrutta la sua possibilità di accedere al sistema informatico al fine di effettuare delle operazioni diverse da quelle per le quali ha ottenuto l'autorizzazione, tiene una condotta analoga a quella di mantenersi nel sistema contro la volontà tacita di colui che ha il diritto di escluderlo e che, pertanto, rientra nella fattispecie prevista e punita dalla seconda parte del comma 1 dell'art. 615

---

[181]Cfr. FLOR R., *Phishing, identify theft e identify abuse: le prospettive applicative del diritto penale vigente,* cit., p. 930.

[182] D'AIUTO G., LEVITA L., *I reati informatici. Disciplina sostanziale e questioni processuali*, Milano, 2012, p. 60 ss.

ter c.p.[183].

Di conseguenza, si configura il reato di accesso abusivo ad un sistema informatico o telematico tutte le volte in cui un soggetto, con la propria condotta, effettua l'accesso senza alcuna autorizzazione fornita dalla vittima ad informazioni contenute nel sistema, al di là del loro carattere personale o meno, rilevando l'intrusione non autorizzata in quanto tale, anche nei casi in cui l'elaboratore non contenga alcun dato[184].

Tuttavia, in tal modo sorge il rischio che l'ordinamento offra tipologie di tutela soltanto formali che spingerebbero ad una censura di incostituzionalità della norma per violazione del principio di proporzione e, per tali ragioni, sarebbe preferibile, in tale settore, l'intervento del legislatore, al fine di selezionare con maggior chiarezza i comportamenti di illecita intrusione nei sistemi informatici protetti.

Appare difficile configurare in un attacco di *phishing* un accesso abusivo il quale non sia seguito da una qualche alterazione o intervento sul sistema informatico oggetto dell'attacco, soprattutto nella fase in cui il *phisher* interviene per nascondere le tracce dell'accesso abusivo realizzato: in tali circostanze, la sua condotta integrerà il reato di frode informatica previsto e punito dall'art. 640 *ter* c.p.

Al riguardo, la Cassazione ha affermato il concorso tra i due reati, poiché gli stessi

---

[183]Cfr. Trib. Nola, sent. 11 dicembre 2007, n. 488, in *www.leggiditalia.it*.

[184]Cfr. Cass. Pen. Sent. 4 ottobre 1999, n. 214945, in *Dir. Inf.,* 2001, p. 485. si tratta della soluzione interpretativa che si adatta meglio alla lettera della legge, in quanto la norma non opera distinzioni tra sistemi a seconda dei contenuti, bensì soltanto delle misure di sicurezza e allo scopo della legge, purché l'interpretazione contraria porterebbe all'esclusione dalla tutela di aspetti non secondari, quali quelli connessi ai profili economico-patrimoniali dei dati.

presentano dei presupposti giuridici diversi[185], nonché in ragione della diversità dei beni giuridici tutelati dal punto di vista dell'elemento soggettivo e per la previsione della possibilità di commettere il reato di accesso abusivo soltanto nei confronti di sistemi protetti, caratteristica non ricorrente nel reato di frode informatica[186]. Il *phishing attack* potrebbe anche essere riconducibile al reato di "*detenzione e diffusione abusiva di codici di accesso a sistemi informatici"*, di cui all'art. 615 *quater* c.p., il quale sanziona penalmente la condotta di colui che, al fine di procurare a sé o ad altri un profitto e arrecare ad altri un danno, si procura codici o altri mezzi idonei all'accesso ad un sistema informatico protetto[187].

Tale condotta può dirsi equivalente a quella del *phisher*. Difatti, quest'ultimo si procura mediante artifici e raggiri – come, ad esempio, mediante l'uso di un *layout* simile o uguale alla potenziale banca del destinatario, o anche tramite l'avvio di un *trojan* in seguito all'accesso da parte della vittima al sito finto – le *password,* i codici cliente, i numeri delle carte di credito e tutto ciò che gli consenta di accedere al conto corrente della vittima.

Le credenziali sono infatti considerate come qualità personali riservate, identificatrici della persona: pertanto, viene punito penalmente il soggetto che si procuri illecitamente tali credenziali al fine di superare i controlli di sicurezza, rischiando di porre in pregiudizio l'integrità, la riservatezza e la disponibilità dei dati[188].

---

[185]Così previsto da Cass. Pen., sent. 24 febbraio 2011, n. 9891, in *www.italgiure.giustizia.it.*

[186]Cfr. Cass. Pen., sent. 1 ottobre 2004, n. 2672, in *www.italgiure.giustizia.it.*

[187] V. Di Lembo, *Il "phishing": dall'illecita captazione di dati alla truffa*, cit., p. 71.

[188] D'AIUTO G., LEVITA L., *I reati informatici. Disciplina sostanziale e questioni processuali*, Milano, 2012, p. 70 ss.

3.1.4 Il furto di identità digitale attraverso il *phishing*

Sebbene nell'ordinamento penale italiano non sussista un reato specifico atto a punire il "furto di identità", l'unica fattispecie penale che si occupa di tale condotta illecita è l'art. 494 c.p., il quale disciplina sia la sostituzione della propria ad altrui persona, sia l'attribuzione a sé o ad altri di un falso nome, un falso stato o una qualità a cui la legge riconosce effetti giuridici in modo tale da indurre altri in errore, al fine di procurare un profitto o di arrecare un danno.

In ragione dell'estensione del concetto di "*qualità cui la legge attribuisce effetti giuridici"*, la nozione di "identità" rilevante ai sensi dell'art. 494 c.p. ricomprende tutti quei dati personali in grado di identificarla, come anche la casella di posta elettronica o gli estremi del conto corrente bancario o postale[189].

Al contrario, nel concetto di "*sostituzione di persona"* può farvisi rientrare anche l'attribuzione a sé di un'immagine o di un video in cui sono ritratti altri soggetti.

La *ratio* sottesa alla punizione di tale condotta non è soltanto la necessità di tutelare il bene giuridico della fede pubblica, ma anche in quanto il fatto si presta alla configurabilità di frodi di vario genere[190].

Il reato previsto e punito dall'art. 494 c.p. presenta natura sussidiaria, come può ricavarsi dalla formula di chiusura "*se il fatto non costituisci altro reato contro la fede pubblica"*. È consentito il concorso con i reati di cui agli artt. 640 e 640 *ter* c.p., in quanto lesivi di un bene giuridico diverso – vale a dire, il patrimonio –

[189] V. Di Lembo, *Il "phishing": dall'illecita captazione di dati alla truffa*, cit., p. 74.

[190] D'AIUTO G., LEVITA L., *I reati informatici. Disciplina sostanziale e questioni processuali*, Milano, 2012, p. 71 ss.

nonché con il reato di cui all'art. 615 *ter* c.p.

Come è già stato anticipato nei precedenti paragrafi della presenta trattazione, nella prima fase del *phishing,* le condotte poste in essere possono configurare il reato di sostituzione di persona, di cui all'art. 494 c.p. Difatti, proprio nella fase iniziale di un *phishing attack*, il soggetto agente, al fine di "pescare" le sue vittime, fa utilizzo di messaggi di posta elettronica ingannevoli, i quali sembrano provenire, in apparenza, da mittenti reali, utilizzando identificativi di organizzazioni realmente esistenti.

Anche la giurisprudenza ha considerato tale attività criminosa come rientrante nella fattispecie penale della sostituzione di persona[191].

Difatti, la condotta descritta nell'art. 494 c.p. integra tutti gli elementi costitutivi richiesti, sia sotto il profilo oggettivo – vale a dire l'induzione in errore della persona offesa tramite la sostituzione illegittima di persona –, sia sotto il profilo soggettivo, ovvero del dolo specifico, poiché l'invio del messaggio di posta elettronica è finalizzato a procurarsi un vantaggio con la produzione di un danno altrui[192].

In una recente pronuncia, la Cassazione ha ritenuto che "*integra il reato di sostituzione di persona, di cui all'articolo 494 c.p., la condotta di colui che crei ed utilizzi un account di posta elettronica, attribuendosi falsamente le generalità di un diverso soggetto, inducendo in errore gli utenti della rete internet, nei confronti dei quali le false generalità siano declinate e con il fine di arrecare danno al*

[191]Cfr. Cass. Pen., sent. 14 dicembre 2007, n. 46674, in *www.leggiditalia.it.*

[192] P. Cipolla, *Social network", furto di identità e reati contro il patrimonio*, in *Giurisprudenza di merito*, 12, 2012, pp. 2672-2696.

soggetto le cui generalità siano state abusivamente spese"[193]*.*

Nei casi in cui il *phisher* assuma l'identità di una persona indeterminata – come nel caso in cui il mittente appaia un organismo, un'istituzione, una società – sembrerebbe che l'ipotesi non possa ricondursi all'ambito applicativo del reato di cui all'art. 494 c.p.[194].

Tuttavia, alcune pronunce della giurisprudenza di merito ha ritenuto la responsabilità penale del *phisher* ai sensi dell'art. 494 c.p. anche per la condotta di invio di false *e-mail*, mediante le quali si ammonivano gli utenti circa presunti problemi di sicurezza relativi agli istituti di credito e la creazione di false pagine *web* – simili in tutto a quelle degli istituti di credito di cui la vittima era cliente – sebbene la persona sostituita fosse indeterminata[195].

Vi è da dire che, al di fuori del sistema penale, l'ordinamento italiano tutela l'identità digitale mediante il c.d. Codice della *privacy* – D. Lgs. 30 giugno 2003, n. 196 – il quale, all'art. 2 afferma che il codice stesso "*garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali".*

In effetti, l'uso non autorizzato dei dati personali o dei documenti di un individuo incide sulla genuinità, integrità e correttezza dei dati personali.

---

[193]Cfr. Cass. Pen., sent. 15 dicembre 2019, n. 12479, in *www.italgiure.giustizia.it.*

[194]Cfr. FLOR R., *Phishing, identiy theft e identify abuse: le prospettive applicative del diritto penale vigente,* cit., p. 903.

[195]Cfr., *ex multis,* Trib. Milano, sent. 7 ottobre 2020, n. 11696.

3.2 Il caso "Poste italiane e Banca Intesa": i reati contestati

La decisione sul caso "*Poste italiane e Banca Intesa"* rappresenta una delle prime nonché più importanti sentenze della giurisprudenza italiana sui c.d. *phishing attacks*[196].

Difatti, la pronuncia del GIP di Milano, dopo una preliminare indagine sul fenomeno, unitariamente inteso, ha affrontato la questione, evidenziandone il carattere "sovranazionale", in ragione della sua manifestazione sul *web* mediante la raccolta illecita di dati personali dell'utente, il loro utilizzo "abusivo" e la realizzazione di un evento "materiale" quale conseguenza causale dei fatti criminosi realizzati in rete[197].

Ripercorrendo i fatti della vicenda, il caso ha riguardo il fatto di più soggetti che, associati tra di loro, hanno costituito un'associazione criminale avente l'obiettivo di realizzare delle truffe finalizzate all'utilizzo indebito di carte di credito di soggetti titolari di conti correnti accesi presso Poste Italiane e Banca Intesa, mediante l'attività di accesso abusivo ai sistemi di *home banking*.

Gli imputati ottennero da tali due istituti l'attivazione di carte di credito e di pagamento – anche in favore di altri soggetti, compartecipi consapevoli, o

[196]Cfr. GIP, Trib. Milano, sent. 10 dicembre 2007, n. 888, in *Rivista di Giurisprudenza ed Economia d'Azienda,* n. 4, 2008, p. 80.

[197]Cfr. PERRI R., *Lo smishing e il vishing, ovvero quando l'unico limite all'utilizzo criminale delle nuove tecnologie è la fantasia,* in *Diritto dell'Internet,* 2008, p. 265.

intestati a persone fittizie – sui quali confluivano i fondi illeciti[198].

In particolare, al fine di procurarsi le credenziali di accesso delle ignare vittime, gli imputati hanno inviato ad un elevato numero di utenti delle false *e-mail* attraverso tecniche di *spam*, simulando la provenienza da parte di reali istituti bancari. Il messaggio di posta elettronica era stato formulato in modo tale da spingere la vittima a visitare una pagina *web* del tutto simile a quella delle Poste Italiane. Inoltre, erano state usate delle *e-mail* appositamente aperte in "funzione di collettori" di credenziali di autenticazione[199].

Dopo aver ottenuto i nomi utenti e le *passwords*, gli imputati avevano effettuato l'accesso, in modo abusivo, agli spazi informatici riservati dai correntisti, svolgendo delle operazioni di ricarica delle carte menzionate, mediante l'uso indebito dei codici di accesso degli utenti ai servizi *on-line.*

Peraltro, alcuni degli accessi abusivi che erano stati effettuati erano avvenuti al solo fine di verificare la consistenza delle carte dei singoli utenti, al fine di procedere al trasferimento dei fondi. Infine, gli imputati avevano ricaricato indebitamente delle carte di credito, identificate con il numero e il nome del titolare abusivamente acquisiti[200].

Di conseguenza, oltre all'associazione a delinquere di cui all'art. 416 c.p., i reati

---

[198] DI LELLA F., *Utilizzo fraudolento di credenziali informatiche nei servizi di "home banking" e responsabilità civile dell'istituto di credito*, in *Il Foro napoletano*, 1, 2015, p. 92 ss.

[199] P. Cipolla, *Social network", furto di identità e reati contro il patrimonio*, cit., p. 2673 ss.

[200] DI LELLA F., *Utilizzo fraudolento di credenziali informatiche nei servizi di "home banking" e responsabilità civile dell'istituto di credito*, in *Il Foro napoletano*, 1, 2015, p. 97 ss.

contestati (realizzati in concorso fra diversi soggetti e mediante più condotte esecutive di un medesimo disegno criminoso) sono stati:

- art. 617 *sexies* c.p. (falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche);
- art. 640 c.p. (truffa);
- art. 615 *ter* c.p. (accesso abusivo a sistema informatico o telematico);
- art. 12 L. 5 luglio 1991, n. 197 (indebito utilizzo di carte di credito e di pagamento).

Nel caso di specie, sono state considerate applicabili anche le aggravanti di cui ai numeri 2 e 7 dell'art. 61 c.p., ovvero, rispettivamente: l'aver commesso il reato per eseguirne od occultarne un altro o per conseguire o assicurare a sé o ad altri il prodotto, il profitto o prezzo, ovvero l'impunità; l'aver cagionato un danno patrimoniale di rilevante gravità nei delitti contro il patrimonio o che offendono il patrimonio o nei delitti determinati da fini di lucro (nel caso di specie, a danno sia del correntista che degli istituti bancari)[201].

Da ultimo, il delitto di associazione per delinquere, nonché i reati di cui agli artt. 615 *ter* c.p. e 12 Legge 5 luglio 1991, n. 197, sono stati ricondotti nella definizione di "reato transnazionale", essendo la relativa preparazione e pianificazione avvenuta ("*per una parte sostanziale*") in Romania.

Difatti, l'art. 3, comma 1, lett. b) della Legge 16 marzo 2006, n. 146 (di ratifica ed esecuzione della convenzione e dei protocolli delle Nazioni Unite contro il crimine

[201] P. Cipolla, *Social network", furto di identità e reati contro il patrimonio*, cit., p. 2677.

organizzato transnazionale, adottati dall'Assemblea Generale il 15 novembre 2000 e il 31 maggio 2001, definisce “reato transnazionale” quello punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto in un gruppo criminale organizzato, nonché sia commesso in uno Stato, mentre una parte sostanziale della sua preparazione, pianificazione, direzione o controllo sia avvenuta in un altro Stato[202].

3.2.1 Argomentazioni giurisprudenziali sul tema controverso

Il giudice di merito – dopo aver proceduto a ripercorrere nel dettaglio la fase delle indagini preliminari, riportandone gli esiti – ha dedicato particolare attenzione alla verifica degli elementi strutturali della fattispecie di cui all'art. 416 c.p., concludendo in merito alla sussistenza della “*formazione e permanenza di un vincolo associativo continuativo tra tre o più persone allo scopo di commettere una serie indeterminata di delitti, con la predisposizione comune dei mezzi occorrenti per la realizzazione del programma e con la permanente consapevolezza di ciascun associato di far parte del sodalizio criminoso”*[203].

Tale arresto positivo è relativo anche all'aggravante contestata e connessa alla categoria del “reato transnazionale”. Nello specifico, l'art. 4 della Legge n. 146/2006 dispone che “*per i reati puniti con la pena della reclusione non inferiore nel massimo a quattro anni nella commissione dei quali abbia dato il suo contributo un gruppo criminale organizzato impegnato in attività criminali in più di*

[202] P. Cipolla, *Social network", furto di identità e reati contro il patrimonio*, cit., p. 2678.

[203] Cfr. GIP, Trib. Milano, sent. 10 dicembre 2007, n. 888, cit.

uno Stato, la pena è aumentata da un terzo alla metà". Nel caso in questione, il giudice di merito ha ritenuto che l'associazione per delinquere rientri tra i delitti cui si riferisce la convenzione e l'aggravante di cui all'art. 4 si applica in conformità ai parametri dello stesso art. 3[204].

Orbene, con riguardo a tali reati fine, la difesa degli imputati aveva ritenuto che si configurasse soltanto la fattispecie di reato prevista e punita dall'art. 640 *ter* c.p., la quale assorbiva tutte le altre ipotesi delittuose contestate.

Al contrario, i giudici hanno ritenuto – avallando le teorie interpretative della dottrina nella materia in esame – che l'elemento oggettivo richiesto da tale fattispecie necessita della realizzazione di una delle condotte tipizzate dalla norma - vale a dire, l'alterazione del funzionamento di un sistema informatico o di un intervento senza diritto su dati, informazioni o programmi ivi contenuti – di fatto non sussistenti.

A ben vedere, il comportamento delittuoso del *phisher* riproduce lo schema dell'induzione in errore del soggetto passivo, rappresentante il tipico modo di operare della fattispecie di reato della truffa[205].

In tal senso, il giudice di merito ha posto in risalto l'evidenza degli artifici e dei raggiri posti in essere da colui che utilizza un messaggio di posta elettronica il quale riproduce i colori, i marchi e le altre caratteristiche distintive di un ente reale.

---

[204] DI LELLA F., *Utilizzo fraudolento di credenziali informatiche nei servizi di "home banking" e responsabilità civile dell'istituto di credito*, in *Il Foro napoletano*, 1, 2015, p. 100.

[205] DI LELLA F., *Utilizzo fraudolento di credenziali informatiche nei servizi di "home banking" e responsabilità civile dell'istituto di credito*, in *Il Foro napoletano*, 1, 2015, p. 101.

Inoltre, sono stati considerati realizzati gli altri elementi costitutivi della fattispecie, compresi il danno e l'ingiusto profitto, oltre alla disposizione patrimoniale.

In particolare, il danno è risultato evidente e di rilevante gravità sia per l'ente – il quale ha subito la clonazione dei propri siti e dei propri segni distintivi – sia per gli stessi correntisti. Pertanto, secondo il giudice, risultano realizzate le aggravanti contestate[206].

Per ciò che attiene agli elementi costitutivi del reato di accesso abusivo a sistema informatico o telematico – soprattutto con riguardo ai sistemi dei titolari di carte di credito e di pagamento e di *home banking* per effettuare operazioni di ricarica sulle stesse carte acquistate dall'organizzazione criminale, il giudice di merito ha concluso affermando la sussistenza del reato, dopo aver ripercorso l'evoluzione degli orientamenti giurisprudenziali in merito alle condotte tipiche di "introduzione" e di "mantenimento", al bene giuridico oggetto di protezione nonché all'ammissibilità del concorso con il reato di truffa *ex* art. 640 c.p.[207].

In particolare, il giudice ha sottolineato che i nomi utenti e le *password* di accesso al sistema informatico presentano la natura di "misura di sicurezza".

Con riguardo alla verifica della sussistenza dei requisiti di cui all'art. 12, Legge n.

---

[206]Cfr. FLOR R., *Phishing, identity theft e identity abuse,* cit., p. 899.

[207]In particolare, il bene giuridico "riservatezza informatica" è costituito dall'interesse esclusivo, giuridicamente riconosciuto, di godere, disporre e controllare le informazioni, i procedimenti, i sistemi e "spazi" informatizzati e le relative utilità. La chiave di volta della fattispecie penale è lo *jus excludendi alios*, inteso quale diritto del titolare di escludere l'accesso indesiderato di terzi dallo spazio informatico di sua pertinenza. Tale diritto si manifesta con la predisposizione di mezzi di protezione, di carattere logico e/o fisico, che rappresentano un elemento obiettivo, la cui violazione prova (o indizia sino a prova contraria) la mancanza di un consenso esplicito o implicito del titolare dello *spatium operandi*., cfr. FLOR R., *Art. 615 ter c.p.: natura e funzioni delle misure di sicurezza, consumazione del reato e bene giuridico protetto,* in *Dir. Pen. Proc.,* 2008, p. 106.

197/1991 (utilizzo indebito di carte di credito o di pagamento), il sistema di trasferimento di denaro da *postepay* a *postepay* consentiva, appunto, la trasmissione di fondi dalla carta dell'utente a quella del *fisher.*

Secondo il giudice è pacifico che, come già posto in evidenza dal Tribunale del riesame di Milano, che tali carte rappresentino dei "*documenti abilitanti al prelievo di denaro contante o all'acquisto di beni o servizi"*. Inoltre, il giudicante ha ritenuto configurato tale reato – in luogo del reato di cui all'art. 640 *ter* c.p. - poiché la condotta del *phisher*, nel caso di specie, è risultata finalizzata a "ricaricare" le menzionate carte mediante l'utilizzo indebito delle credenziali del legittimo titolare, sottratte in via fraudolenta a chi le deteneva stabilmente[208].

Dal punto di vista, invece, del rapporto con il reato di truffa comune, la diversità dell'elemento oggettivo e del bene giuridico protetto ha spinto il giudice a ritenere la configurazione del concorso formale di reati. Ed infatti, sotto l'aspetto oggettivo, l'art. 12 della legge in commento – a differenza di quanto previsto nell'art. 640 c.p. - punisce penalmente la condotta di utilizzo indebito di carta di credito o di pagamento a prescindere dal conseguimento di un profitto e dalla verificazione di un danno[209].

Peraltro, la condotta in questione è indipendente dal necessario utilizzo di artifici o di raggiri che spingano il soggetto in errore.

Con riguardo al bene protetto, mentre la truffa si caratterizza per essere un classico delitto che offende il patrimonio, il reato di cui all'art. 12 della Legge 5

---

[208] Cfr. FLOR R., *Phishing, identity theft e identity abuse,* cit., p. 935.

[209] DI LEMBO V., *Il "phishing": dall'illecita captazione di dati alla truffa*, in *Rassegna dell'Arma dei Carabinieri*, 4, 2013, p. 19 ss.

luglio 1991, n. 197 si pone a tutela dell'interesse pubblico al corretto utilizzo del sistema di pagamento, a garanzia della fede pubblica e della prevenzione del riciclaggio[210].

[210]Cfr. GIP di Milano nella sentenza in esame, il quale riprende un orientamento della giurisprudenza di legittimità. Si veda in proposito Cass Pen., sent. 8 marzo 2006, in *Cass. Pen.,* 2007, p. 720.

Ma vi è di più. Il giudice si è anche preoccupato di affrontare la questione relativa al concorso apparente di norme e di reati fra le disposizioni normative richiamate, riproducendo gli orientamenti giurisprudenziali in materia.

Difatti, da una parte, gli artifici o i raggiri rappresentano uno dei modi mediante i quali si manifesta l'uso indebito delle carte di credito e di pagamento, mentre, dall'altra, si consente il concorso di reati allorquando la condotta del reo non si limiti a tale utilizzo, bensì sia connotata da un *quid pluris* di attività ingannatoria[211].

In buona sostanza, oltre a quanto esposto, la truffa non può dirsi assorbita nel più grave reato costituito dall'indebito utilizzo di carte di credito o di pagamento, difettando l'identità del bene giuridico alla cui tutela sono finalizzate le disposizioni in commento[212].

Peraltro, è stato ritenuto configurabile anche l'art. 617 *sexies* c.p. con riguardo alla condotta di formazione del contenuto non veritiero di un messaggio di posta elettronica, proveniente in apparenza da enti o istituzioni reali. Anche in tal caso, il giudice ha fatto utilizzo del criterio della “diversità del bene giuridico” al fine di affermare il possibile concorso con il reato di cui all'art. 640 c.p., sostenendo che l'art. 617 *sexies* c.p. si ponga a tutela dell'“*integrità della comunicazione telematica nelle forme di autenticità della comunicazione, della conformità del contenuto originale e della esistenza stessa della comunicazione”.*

---

[211] DI LEMBO V., *Il "phishing": dall'illecita captazione di dati alla truffa*, in *Rassegna dell'Arma dei Carabinieri*, 4, 2013, p. 33 ss.

[212]Cfr. PITTARO, *Indebito utilizzo di una carta di credito e truffa: concorso di reati o concorso apparente?,* in *Dir. Pen. Proc.,* 1995, p. 945.

3.3 La Legge di ratifica della Convenzione *Cybercrime*

La mancanza, nell'ordinamento giuridico italiano, di una norma che sanzioni nello specifico il fenomeno del *phishing*, ha spinto la dottrina, prima ancora della giurisprudenza, ad analizzare le prospettive applicative del diritto vigente[213].

Dal punto di vista metodologico, gli attacchi di *phishing* sono stati suddivisi in più fasi al fine di comprendere quali di esse assumano rilevanza penale.

La sentenza in esame presenta il pregio di aver approfondito alcune importanti questioni interpretative, anche con riguardo alla categoria dei "reati transnazionali", inserita nell'ordinamento ad opera della Legge 16 marzo 2006, n. 146. Nello specifico, il giudice ha motivato l'applicazione del delitto di associazione per delinquere e dei reati di cui agli artt. 640 c.p. e 12 L. n. 197/1991, nonché i rapporti tra tali due norme[214].

Tuttavia, il giudice ha ritenuto la sussistenza dei reati di accesso abusivo a sistemi informatici o telematici, individuando il bene giuridico nel c.d. domicilio informatico, senza considerare l'evoluzione ermeneutica della dottrina in tale materia.

In secondo luogo, il giudice non ha motivato compiutamente l'applicazione del reato di cui all'art. 617 *sexies* c.p. il quale, proprio in ragione dell'assenza di importanti precedenti giurisprudenziali, richiedeva maggiore attenzione.

A questo punto, occorre dedicare un breve riflessione alle novità introdotte dalla

---

[213]FLOR R., *Phishing, identity theft e identity abuse,* cit., p. 899.

[214] DI LEMBO V., *Il "phishing": dall'illecita captazione di dati alla truffa*, in *Rassegna dell'Arma dei Carabinieri*, 4, 2013, p. 46 ss.

L. 16 marzo 2006, n. 146, nonché alle prospettive applicative del diritto penale al fenomeno del *phishing* a seguito della legge di ratifica della Convenzione *Cybercrime*, L. 18 marzo 2008, n. 48.

Quest'ultima normativa è intervenuta in quattro "macro settori":

- codice penale;
- codice di procedura penale;
- D.lgs 30 giugno 2003, n. 196 (c.d. "Codice Privacy");
- D.lgs 8 giugno 2001, n. 231 ("Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300")[215].

Dal punto di vista del diritto penale sostanziale, la legge ha operato su tre livelli, prevedendo nuove fattispecie incriminatrici, abrogando alcune disposizioni normative e modificandone altre[216].

Alla luce delle nuove disposizioni, qualora i *phishing attacks* determinino la distruzione, il danneggiamento, o rendano, in tutto o in parte, inservibili sistemi informatici o telematici altrui, o ne ostacolino gravemente il funzionamento ovvero procurino la cancellazione, la distruzione, l'alterazione, la soppressione o il deterioramento dei dati e delle informazioni in essi contenuti, in base alla natura di pubblica utilità o meno dei dati (o se siano o meno utilizzati dallo Stato o da

[215]Cfr. PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale,* in *Dir. Pen. Proc.,* 2008, n. 6, p. 700.

[216] P. Cipolla, *Social network", furto di identità e reati contro il patrimonio*, cit., p. 2678.

altri enti pubblici) o dei sistemi in questione, sono astrattamente configurabili gli illeciti previsti dagli artt. 635 *bis* c.p. (Danneggiamento di informazioni, dati e programmi informatici), 635 *ter* c.p. (Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità), 635 *quater* c.p. (Danneggiamento di sistemi informatici o telematici) e 635 *quinquies* c.p. (Danneggiamento di sistemi informatici o telematici di pubblica utilità)[217].

Inoltre, la legge di ratifica ha introdotto nel sistema penale l'art. 495 *bis* c.p. (rubricato "Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri"). Si tratta di una fattispecie astrattamente applicabile ai casi di *phishing attacks*, soprattutto qualora l'agente fornisca, in ogni modo, false generalità al certificatore al fine di poter utilizzare abusivamente i profili identitari altrui anche tramite documenti informatici "sottofirmati" con firma elettronica.

Potrebbe sicuramente applicarsi anche il delitto di "frode informatica del soggetto che presta servizi di certificazione di firma elettronica", previsto dal nuovo art. 640 *quinquies* c.p., il quale sanziona penalmente il "*soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato*"[218].

---

[217]In tal senso si veda PICOTTI, *Ratifica della Convenzione Cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo*, in *Dir. dell'Internet*, 5, 2008, p. 437.

[218]Nel caso, si configurerebbe il reato se il certificatore, a seguito della promessa, da parte di un soggetto che partecipi alla realizzazione del fatto criminoso, di ricevere un compenso, non provveda con certezza all'identificazione della persona che fa richiesta della certificazione, oppure non assicuri la precisa determinazione della data e dell'ora di rilascio del certificato

Da ultimo, l'art. 4 della L. 18 marzo 2008, n. 48 ha sostituito l'originaria disposizione prevista dall'art. 615 *quinquies* c.p. con quella di "*Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematici*", la quale punisce penalmente la condotta di colui che, al fine di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici.

La norma menzionata trova certamente applicazione nel caso in cui, per ipotesi, vengano messi a disposizione dei *kit* per i *phishing attacks*, se sussiste l'elemento soggetto finalistico del reato.

Un'ulteriore novità introdotta con la legge di ratifica della Convenzione Cybercrime riguarda le modifiche al D. Lgs 8 giugno 2001 n. 231, in cui è stato introdotto l'art. 24 *bis* che estende la responsabilità dell'ente anche per tutti i reati informatici (salvo che per quelli di cui agli artt. 495 *bis* e 640 *ter*, ipotesi base, c.p.). Tale disposizione normativa rileva in caso di illeciti commessi da *insiders* (dipendenti infedeli), anche se in concorso con *outsiders* (soggetti esterni), purché ne derivi un vantaggio, anche minimo o solo indiretto, all'ente.

---

elettronico o, ancora, non tenga registrazione di tutte le informazioni relative al certificato qualificato. Il certificatore, infatti, è responsabile dell'identificazione del soggetto che richiede il certificato e deve raccogliere i dati personali solo presso la persona cui essi si riferiscono, o previo suo consenso, e solo nella misura necessaria al rilascio ed al mantenimento del certificato (fornendo l'informativa al trattamento dati prevista dall'art. 13 del D.lgs 30 giugno 2003, n. 196).

In merito alla L. 16 marzo 2006, n. 146 (di ratifica ed esecuzione della convenzione e dei protocolli delle Nazioni Unite contro il crimine organizzato transnazionale, adottati dall'assemblea generale il 15 novembre 2000 ed il 31 maggio 2001), essa ha introdotto nell'ordinamento giuridico italiano una nuova categoria, il "reato transnazionale"[219].

Nel caso in questione, il giudice ha ritenuto (correttamente) che la partecipazione ad un gruppo criminale organizzato volto alla commissione di reati in Italia, ma aventi una parte sostanziale della relativa preparazione e pianificazione in Romania, integri il carattere "transnazionale" dell'illecito, ai sensi e per gli effetti dell'art. 3, co. 1, lett. b) L. 16 marzo 2006, n. 146.

Pertanto, la sentenza del giudice di Milano, giungendo in un periodo di riforme sostanziali del diritto penale dell'informatica, oltre che successivamente alla ratifica della citata convenzione delle Nazioni Unite contro il crimine organizzato transnazionale, acquista ancor più rilevanza, considerando che ha ritenuto applicabili al fenomeno del *phishing*, da una parte, le nuove norme previste dalla L. 16 marzo 2006, n. 146 e, dall'altro lato, disposizioni penali anteriori alla legge di ratifica della Convenzione *Cybercrime*.

[219]ASTROLOGO C., *Prime riflessioni sulla definizione di reato transnazionale nella Legge n. 146/2006,* in *Cass. Pen.,* 2007, p. 1789.

3.4 *phishing* bancario: orientamenti giurisprudenziali

Si è detto come il *phishing* bancario sia una delle modalità più frequenti di realizzazione di tale fenomeno di *cybercrime*. Esso, in buona sostanza, consiste in una truffa attraverso la quale soggetti terzi, facendo uso di diverse tecniche di raggiro, sono in grado di entrare in possesso dei codici di accesso al conto di un cliente e, di conseguenza, sottrarre le somme in esso presenti[220].

In considerazione del fatto che, di frequente, diviene particolarmente difficoltoso rintracciare l'autore del *phishing*, l'azione del truffato si sposti nei confronti dell'istituto bancario, al fine di ottenere il rimborso delle somme fraudolentemente sottratte.

Al riguardo, l'istituto bancario risponde, a condizione che non vi sia colpa grave del cliente: la valutazione in merito a tale elemento è soggetta a margini di discrezionalità particolarmente ampi e, di conseguenza, non risulta sempre agevole fornire delle valide indicazioni.

Tuttavia, accade spesso che il *phishing* si ponga in essere mediante la cooperazione del cliente, il quale clicca su link inviati via email o SMS quando è evidente che non provengano dalla propria banca o quando è noto che la banca non li richiede per accedere.

In proposito, si discute sulla corretta individuazione della linea di confine tra errore scusabile e colpa grave.

Una decisione del Tribunale di Milano[221] rappresenta un esempio significativo

[220] DI LEMBO V., *Il "phishing": dall'illecita captazione di dati alla truffa*, in *Rassegna dell'Arma dei Carabinieri*, 4, 2013, p. 46.

[221] Tribunale Milano, 07 ottobre 2011.

delle sfide interpretative e applicative relative a casi di phishing. Nel contesto della truffa, l'elemento ingannatorio previsto dall'articolo 640 del Codice Penale richiede quattro elementi chiave: l'inganno, un atto di disposizione patrimoniale (che è un requisito implicito ma fondamentale per il reato), il danno e un profitto ingiusto. È importante notare che la semplice comunicazione delle credenziali di accesso ai sistemi di home banking non costituisce un atto di disposizione patrimoniale completo[222].

Tuttavia, se un terzo soggetto, al di fuori di una situazione di complicità nel reato, contribuisce al successo dell'attacco di phishing sostituendo o trasferendo denaro o altri beni ottenuti attraverso reati dolosi commessi dal "phisher" (come truffa, frode informatica, accesso abusivo a sistemi informatici o diffusione abusiva di codici di accesso), o compie altre azioni per ostacolare l'identificazione dell'origine criminale dei fondi, questo può costituire il reato di ricettazione e riciclaggio.

Per quanto riguarda l'elemento soggettivo richiesto dall'articolo 648-bis del Codice Penale, esso richiede che il soggetto abbia la consapevolezza generica dell'origine criminale del denaro, del bene o delle altre utilità e abbia l'intenzione di ostacolarne l'identificazione. Questo elemento soggettivo può essere compatibile con la forma di dolo eventuale, ma deve basarsi su circostanze oggettive chiare e inequivocabili, e non solo su sospetti vaghi[223].

Il Tribunale di Milano, dopo aver spiegato in modo conciso il fenomeno del

---

[222] R. Flor, *Phishing e profili penali dell'attività illecita di "intermediazione" del cd. financial manager*, in *Diritto penale e processo*, 2012, p. 55 ss.

[223] DI LEMBO V., *Il "phishing": dall'illecita captazione di dati alla truffa*, in *Rassegna dell'Arma dei Carabinieri*, 4, 2013, p. 60.

phishing, ha cercato inizialmente di individuare quali reati penali fossero applicabili alle azioni compiute dal "phisher" (colui che esegue il phishing).

Nel caso specifico, sono stati ipotizzati principalmente tre reati: la sostituzione di persona (articolo 494 del Codice Penale), l'accesso abusivo a sistemi informatici o telematici (articolo 615-ter del Codice Penale) e la truffa comune (articolo 640 del Codice Penale)[224].

Nel dettaglio, nel caso in questione, il reato alla base delle accuse di ricettazione e riciclaggio è stato individuato nella truffa comune. Il "phisher," utilizzando inganni come l'invio di e-mail e la creazione di pagine web false, ha ingannato gli utenti, spingendoli a fornire le proprie credenziali per accedere ai loro conti correnti. Il profitto illegale e il danno subito da altri sono derivati dalle somme "sottratte" illegalmente da questi account.

Per quanto riguarda il ruolo del "financial manager" (il gestore finanziario), il Tribunale ha fatto una distinzione tra due scenari:

1. Se il financial manager agisce consapevolmente, cioè sa della natura fraudolenta complessiva delle attività del "phisher," dovrebbe essere accusato di complicità nei reati commessi dal "phisher."

2. Viceversa, se il financial manager agisce senza conoscenza dei fatti commessi a danno dei correntisti, dovrebbe essere accusato dei reati di riciclaggio o ricettazione[225].

[224] R. Flor, *Phishing e profili penali dell'attività illecita di "intermediazione" del cd. financial manager*, cit., p. 60.

[225] R. Flor, *Phishing e profili penali dell'attività illecita di "intermediazione" del cd. financial manager*, cit., p. 63.

Il Tribunale ha ritenuto che quest'ultima situazione fosse quella configurata nel caso specifico. In altre parole, gli imputati sono stati accusati non di essere stati consapevoli dell'intera attività fraudolenta del "phisher," ma piuttosto di aver ricevuto denaro sapendo che proveniva da attività criminale, e in alcuni casi, di averlo trasferito all'estero in modi che ne ostacolavano l'identificazione della provenienza illecita.

In una recente sentenza del Giudice di Pace di Treviso del 2021 sul *phishing* bancario, la giurisprudenza di merito ha affermato che, ai sensi dell'art. 10 D.Lgs. n. 10/2011, tutte le volte in cui l'utente di un servizio di pagamento escluda di aver autorizzato un'operazione di pagamento la quale è stata invece eseguita, spetta al prestatore dei servizi di pagamento fornire la prova che l'operazione in questione è stata autenticata e correttamente contabilizzata, non essendo intervenuto alcun malfunzionamento delle procedure utili per la sua esecuzione o altri inconvenienti[226].

La sentenza in questione aggiunge poi che le perdite che derivano da operazioni di pagamento non autorizzate gravano sull'utente del servizio nel caso in cui lo stesso abbia attutato una condotta fraudolenta o sia inadempiente, con dolo o colpa grave, agli obblighi di cui all'art. 7 del D.Lgs. n. 10/2011, il quale prevede l'uso dello strumento di pagamento conformemente alle regole sull'emissione e l'uso, nonché la celere comunicazione al prestatore di servizi di pagamento del furto, dell'appropriazione indebita o dell'uso non autorizzato dello strumento non appena viene a conoscenza di ciò DI LEMBO V., *Il "phishing": dall'illecita*

[226] Cfr. Giudice di Pace di Treviso, sent. 16 settembre 2021, n. 963, in *www.sistemapenale.it.*

captazione di dati alla truffa, in *Rassegna dell'Arma dei Carabinieri*, 4, 2013.[227].

Pertanto, i giudici escludono la responsabilità (contrattuale) dell'istituto bancario in caso di operazioni poste in essere attraverso strumentazione elettronica, nel caso in cui vi sia colpa grave dell'utente e che rientra nel tipico rischio professionale del prestatore dei servizi di pagamento, prevedibile ed evitare con adeguate misure volte alla verifica della riconducibilità delle operazioni alla volontà del cliente, la possibilità di usare i codici di accesso al sistema da parte dei terzi, non attribuibile al dolo del titolare o alle condotte incaute da non poter essere fronteggiate in anticipo.

Sempre sulla tematica, il Tribunale di Parma[228], con sentenza del 2018, aveva già affermato che, in caso di bonifici effettuati in maniera illecita su conti correnti *online*, ponendo in essere modalità fraudolente finalizzate a rubare codici di protezione e a sottrarre somme di denaro, la prova del corretto funzionamento del sistema – vale a dire la riconducibilità dell'operazione realizzata al correntista che l'ha disconosciuta – grava sull'istituto bancario, facendo applicazione del noto principio di ripartizione dell'onere della prova in tema di responsabilità contrattuale.

La diligenza cui è tenuto l'istituto bancario è quella dell'operatore professionale (*bonus nummarius*). Inoltre, la corretta operatività del servizio bancario attraverso il collegamento telematico – corrispondente ad un interesse dell'istituto di credito stesso – è da ricondurre a pieno titolo nel rischio d'impresa: pertanto, grava sulla

---

[227] DI LEMBO V., *Il "phishing": dall'illecita captazione di dati alla truffa*, in *Rassegna dell'Arma dei Carabinieri*, 4, 2013, p. 61.

[228] Cfr. Trib. Parma, sent. 6 settembre 2018, n. 1268, in *www.italgiure.giustizia.it.*

banca la responsabilità oggettiva, a meno che la stessa non fornisca prova, anche in via presuntiva, che le operazioni contestate dal cliente sono riconducibili allo stesso.

Altra giurisprudenza di merito ha ritenuto, nel 2020[229], che in materia di *phishing* posto in essere con problemi di collegamento all'*home banking*, l'istituto di credito che non si sia adeguato al sistema di sicurezza considerato idoneo in quel momento dalla Banca d'Italia, è tenuto alla restituzione di quanto è stato illegittimamente sottratto nel conto corrente.

In particolare, nella vicenda sottoposta all'attenzione del giudicante, si tratta di un bonifico bancario dell'importo di 5.000,00 euro, non disposto dal cliente: il sistema di sicurezza dell'istituto bancario in questione non prevedeva una *password* aggiuntiva rispetto a quella necessaria per poter accedere, le operazioni di disposizione monetaria venivano notificate alla clientela via *email* e non mediante SMS, più immediati e letti con maggior frequenza rispetto alla posta elettronica[230].

Vanno infine menzionate due recenti pronunce. Nella sentenza n. 6395/2022 la Cassazione ha statuito che risponde del reato di riciclaggio chi mette a disposizione degli hackers il proprio conto per far depositare somme derivanti da attività di frode informatica. In particolare, secondo i giudici «integra il delitto di riciclaggio la condotta di chi, senza aver concorso nel delitto presupposto, metta a disposizione il proprio conto corrente per ostacolare la provenienza delittuosa delle somme da altri ricavate dall'illecita attività di phishing e quindi dalla

[229] Cfr. Trib. Arezzo, sent. 8 aprile 2020, n. 272, in *www.sistemapenale.it.*

[230] DI LEMBO V., *Il "phishing": dall'illecita captazione di dati alla truffa*, in *Rassegna dell'Arma dei Carabinieri*, 4, 2013, p. 65 ss.

commissione del reato di frode informatica, consentendo che sul proprio conto venissero bonificate le somme»[231].

La seconda sentenza è la n. 2682/2022: nell'occasione la Cassazione ha chiarito che la sola titolarità di una Postepay su cui vengono accreditate somme sottratta tramite phishing non comporta di per sé la responsabilità a titolo di frode informatica. In particolare, ad avviso dei giudici, «in assenza di ulteriori elementi indiziari, la semplice titolarità della Postepay beneficiaria dell'illecito accredito non è sufficiente a dimostrare la penale responsabilità in ordine al reato di frode informatica, essendo necessario accertare se il predetto titolare sia responsabile dell'invio della mail o del sms contenente il link che ha reso possibile l'abusiva intromissione nel sistema informatico»[232].

Nel caso di specie una persona è stata accusata di frode informatica dopo aver ricevuto, su una carta Postepay a suo nome, una somma di denaro sottratta illegalmente dal conto corrente di un'altra persona tramite una tecnica di phishing[233].

Inizialmente, sia il tribunale di primo grado che quello d'appello hanno ritenuto l'imputato colpevole sulla base del fatto che la somma sottratta era stata accreditata sulla sua carta Postepay, anche se l'operazione era stata effettuata solo a livello informatico. Di conseguenza, è stata condannata a sette mesi di reclusione per il reato di frode informatica.

---

[231] Cassazione penale sez. II, 02/12/2022, n.6395, in *Guida al diritto*, 2023, 16.

[232] Cassazione penale sez. II, 28/10/2022, n.2682, in Diritto & Giustizia 2023, 24 gennaio (nota di: Attilio Ievolella.

[233] CASSANO G., SCORZA G., VACIAGO G., *Diritto dell'internet,* Milano, 2012, p. 19 ss.

Tuttavia, il legale dell'imputato ha presentato un ricorso in Cassazione sostenendo che la valutazione della corte d'appello era insoddisfacente. Secondo il suo avvocato, non è sufficiente basarsi semplicemente sulla "presenza" della somma sottratta su una carta intestata all'imputato per dimostrare la sua colpevolezza. L'avvocato ritiene che sia fondamentale identificare la persona che ha inviato il link che ha portato al trasferimento di denaro.

La difesa sostiene che bisogna prima individuare il mittente del link prima di attribuire la responsabilità all'imputato come beneficiaria del trasferimento. La Corte di Cassazione ha accolto le obiezioni dell'avvocato dell'imputato, sottolineando che la responsabilità della donna è stata dedotta solamente dalla sua titolarità della carta Postepay che ha ricevuto il denaro dal conto corrente della vittima. Questo, però, non è sufficiente per dimostrare che l'imputato sia l'autore dell'accesso illegale al conto corrente della vittima e dell'invio del link che ha portato alla truffa del phishing[234].

Di conseguenza, l'accusa contro l'imputata è stata definitivamente respinta. Questo è avvenuto in virtù del principio secondo il quale la semplice detenzione della carta Postepay utilizzata per ricevere il denaro illecitamente non è sufficiente a dimostrare la sua responsabilità penale per il reato di frode informatica.

È essenziale, invece, stabilire se il titolare della carta è effettivamente la persona responsabile dell'invio della mail o del messaggio contenente il link che ha permesso l'accesso non autorizzato al sistema informatico del conto corrente della vittima della truffa. In assenza di prove o indizi aggiuntivi, l'imputata è stata

[234] CASSANO G., SCORZA G., VACIAGO G., *Diritto dell'internet,* Milano, 2012, p. 33 s.

quindi scagionata dalle accuse.

CAPITOLO IV
Educare ed informare per una consapevolezza digitale

4.1 Il ruolo di ChatGPT: lo sviluppo dirompente delle nuove tecnologie con tecniche sempre più evolute

Il ruolo di ChatGPT e di tecnologie simili nel contesto dello sviluppo dirompente delle nuove tecnologie con tecniche sempre più evolute è affascinante ed estremamente rilevante. Queste tecnologie basate sull'intelligenza artificiale rappresentano un punto cruciale nel panorama dell'innovazione, in quanto possono contribuire in molteplici modi a guidare e facilitare lo sviluppo di tecnologie sempre più avanzate. Tale strumento può essere utilizzato, a seconda dei punti di vista, sia come strumento di attacco che di difesa.

ChatGPT è un software sviluppato da OpenAI che ha la capacità di simulare conversazioni con esseri umani e generare testi in modo autonomo. Questa tecnologia offre diversi vantaggi, tra cui la capacità di creare testi autentici e ben scritti in base a specifiche richieste[235].

Una delle principali caratteristiche di ChatGPT è la sua capacità di produrre testi che possono facilmente sembrare scritti da esseri umani, il che lo rende utile in numerose situazioni legittime, come la creazione di contenuti per il web o la risposta a domande degli utenti. Inoltre, l'IA può contribuire a ridurre gli errori grammaticali e ortografici nei testi, migliorando così la qualità complessiva delle comunicazioni e delle email che vengono utilizzate per il phishing.

Per affrontare questa problematica, EUROPOL e le forze dell'ordine raccomandano diverse azioni. Prima di tutto, è importante sensibilizzare il

[235] D. Fadda, *Phishing, le nuove tattiche: kit tramite ChatGPT e frodi sui social*, in https://www.cybersecurity360.it/nuove-minacce/phishing-le-nuove-tattiche-kit-tramite-chatgpt-e-frodi-sui-social/, 2023.

pubblico sui rischi connessi all'abuso dell'IA per scopi fraudolenti. Inoltre, le forze dell'ordine e gli operatori del settore dovrebbero ricevere formazione adeguata a comprendere le potenzialità e le sfide dell'IA e come affrontare i reati informatici correlati. Infine, è essenziale investire in meccanismi di sicurezza avanzati per rilevare e prevenire l'abuso dell'IA, al fine di proteggere le persone e le organizzazioni da comportamenti illegali.

In conclusione, sebbene l'IA come ChatGPT offra vantaggi legittimi, è imperativo utilizzarla in modo etico e responsabile e rispettare le leggi in materia di sicurezza informatica. L'abuso di queste tecnologie per scopi illegali non è solo inaccettabile ma può anche comportare gravi conseguenze legali[236].

4.2 Un'educazione digitale per una maggior consapevolezza

L'Agenzia dell'Unione Europea per la CyberSicurezza, conosciuta come ENISA, svolge un ruolo essenziale nella promozione della sicurezza informatica nell'Unione Europea e nei suoi Stati membri. Sebbene ENISA si concentri su diverse aree della cybersicurezza, uno dei suoi compiti chiave è affrontare il problema del phishing.

ENISA fornisce risorse e orientamenti per aiutare sia le organizzazioni che gli individui a difendersi da questo tipo di attacco. Uno dei principali contributi di ENISA è la creazione di materiali educativi come rapporti, linee guida e migliori pratiche. Questi materiali mirano a sensibilizzare le persone sui rischi del

[236] D. Fadda, *Phishing, le nuove tattiche: kit tramite ChatGPT e frodi sui social*,

phishing e a insegnare loro come riconoscerlo e prevenirlo.

Inoltre, ENISA promuove la collaborazione tra diverse parti interessate, come le agenzie di sicurezza informatica nazionali, le forze dell'ordine e le aziende private, per affrontare congiuntamente il phishing e altre minacce alla sicurezza informatica.

L'agenzia fornisce anche orientamenti su come rispondere agli incidenti di phishing, inclusi processi di segnalazione e indagine. Monitorando costantemente l'evoluzione delle minacce di phishing, ENISA condivide informazioni e analisi di intelligence sulle minacce con i suoi partner per mantenere tutti informati sulle minacce emergenti.

Infine, ENISA organizza esercitazioni e simulazioni di cybersicurezza per consentire a organizzazioni e individui di praticare le loro risposte agli attacchi di phishing in un ambiente sicuro e controllato[237].

Complessivamente, il ruolo di ENISA nella lotta al phishing è parte integrante della sua missione di migliorare la sicurezza informatica nell'Unione Europea. Attraverso la sensibilizzazione, la collaborazione e la condivisione di conoscenze, ENISA contribuisce agli sforzi collettivi per proteggere le persone e le organizzazioni dagli effetti dannosi degli attacchi di phishing.

Come noto, viviamo nell’era della dimensione digitale, ogni aspetto della nostra vita quotidiana è pervaso da internet.

Siamo cittadini di un mondo connesso, abbiamo strumenti intelligenti che ci consentono di personalizzare e ottimizzare le nostre esperienze.

Ma perché possiamo utilizzare tutto ciò al meglio, è necessario disporre di idonee

[237] D. Fadda, *Phishing, le nuove tattiche: kit tramite ChatGPT e frodi sui social*,

competenze.

Educare significa informare e formare, giacché la frequentazione di ambienti digitali senza il possesso di adeguate competenze può determinare situazioni di disagio e anche di pericolo e il rischio più comune è proprio quello del phishing.

L'obiettivo, oggi, è quello di acquisire una cittadinanza digitale.

Il cittadino digitale deve avere specifiche competenze per agire efficacemente a tutela della propria e altrui sicurezza, soprattutto perché il mondo digitale influenza anche la vita quotidiana off line.

Le competenze della sicurezza digitale hanno anche conseguenze rilevanti dal punto di vista economico. Il livello di sicurezza digitale influenza la partecipazione dei consumatori e lo sviluppo dei servizi e dei mercati digitali.

Prima di intraprendere un'educazione digitale, sarebbe utile fare test di autovalutazione al fine di comprendere il livello di formazione digitale posseduto.

Occorre interrogarsi sui seguenti aspetti:

Utente base: Posso prendere accorgimenti per proteggere i miei dispositivi (ad esempio, utilizzando antivirus e password)? So che non tutte le informazioni online sono affidabili? So che le mie credenziali (username e password) possono essere rubate? So che non devo rivelare informazioni private online? So che l'eccessivo utilizzo di tecnologia digitale può influenzare negativamente la mia salute? Adotto le misure fondamentali per il risparmio energetico?

Utente autonomo: Ho installato i programmi di sicurezza sul dispositivo che uso per accedere a Internet (ad esempio antivirus, firewall)? Utilizzo questi programmi e li aggiorno regolarmente? Uso diverse password per accedere a dispositivi e servizi digitali e le modifico periodicamente? So identificare i siti o

messaggi di posta elettronica utilizzati per truffa? So identificare una e-mail di phishing (cioè, di truffa via Internet)? Posso modificare la mia identità digitale e tenere traccia della mia impronta digitale? Capisco i rischi sanitari connessi con l'uso della tecnologia digitale (ergonomia, rischio di dipendenza)? Capisco l'impatto positivo e negativo della tecnologia sull'ambiente?

Utente avanzato: Controllo frequentemente la configurazione e i sistemi di sicurezza dei dispositivi e/o delle applicazioni che uso? So come intervenire se il computer è stato infettato da un virus? Posso configurare o modificare le impostazioni del firewall e di sicurezza dei miei dispositivi digitali? So come crittografare e-mail o file? Posso applicare filtri per le e-mail (spam)? Per evitare problemi di salute (fisica e psicologica), faccio un uso ragionevole delle tecnologie dell'informazione e della comunicazione? Ho un parere informato sull'impatto delle tecnologie digitali sulla vita di tutti i giorni, il consumo online e l'ambiente?

Inoltre, erroneamente crediamo che le nostre azioni nell'ambiente digitale non portino conseguenze nel mondo "reale"; invece, è importante acquisire la consapevolezza che il nostro modo di abitare la Rete concorre a caratterizzare la nostra reputazione.

Se utilizziamo la Rete, quasi certamente anche noi abbiamo lasciato delle impronte: siamo diventati un "personaggio pubblico" nel momento in cui abbiamo condiviso nel Web nostre foto o post.

Anche per questo motivo bisogna acquisire la consapevolezza del contenuto dei dati che immettiamo in rete.

Ed infatti, se prima abbiamo parlato di educazione e formazione circa gli

strumenti che ci permettono di navigare, corre l'obbligo di autovalutarsi e formarsi anche sulla nostra capacità di proteggere la nostra privacy.

Il modello europeo DigComp individua due competenze digitali specifiche indispensabili per abitare in sicurezza la dimensione digitale:

▪ proteggere i dati personali e la privacy (sapere in che modo utilizzare e condividere dati personali proteggendo sé stessi e gli altri da eventuali danni; essere a conoscenza che i servizi digitali utilizzano una privacy policy per informare sull'utilizzo che verrà fatto dei dati personali);

▪ gestire l'identità digitale (creare e gestire una o più identità digitali, essere in grado di proteggere la propria reputazione, occuparsi dei dati prodotti mediante l'uso di diversi strumenti digitali, ambienti e servizi[238]).

Con riferimento alla privacy, occorre interrogarsi sui seguenti aspetti:

Utente base: Sono consapevole dei benefici e dei rischi connessi al possesso di un'identità digitale? Quando agisco in un ambiente digitale sono consapevole che le persone possono formarsi un'idea su di me o su altri attraverso ciò che condivido? Negli ambienti digitali condivido informazioni che riguardano me e/o altri rispettando le principali norme sulla privacy?

[238] AgID ha focalizzato le proprie attività nella valorizzazione dei modelli europei per la catalogazione delle competenze digitali di base. Il 15 febbraio 2018 si è conclusa la consultazione pubblica della prima versione della traduzione ufficiale in lingua italiana del modello europeo DigComp 2.1. Anche in questo caso, AgID è la prima realtà governativa in Europa a curare direttamente la traduzione ufficiale di tale modello.
https://www.agid.gov.it/sites/default/files/repository_files/digcomp2-1_ita.pdf
https://competenze-digitali-docs.readthedocs.io/it/latest/doc/competenze_di_base/Intro_Modello_Europeo_DigComp_2_1.html

Utente autonomo: Costruisco in modo consapevole la mia identità e reputazione digitale, verifico con costanza le mie impronte online? Sono in possesso di conoscenze di base relative a come, negli ambienti digitali, i miei dati sono raccolti e per quali finalità possono essere utilizzati? Leggo con attenzione l'informativa relativa al trattamento dei dati fornita dagli enti/società che gestiscono gli ambienti digitali in cui interagisco?

Utente avanzato: Gestisco identità digitali in diversi ambienti e per diverse finalità? Monitoro le informazioni che produco nella mia interazione online? Proteggo in modo attivo la mia reputazione digitale monitorando le interazioni di altri soggetti (ad esempio controllo tag, foto e conversazioni)? Cambio frequentemente le impostazioni preimpostate negli ambienti digitali per personalizzare e/o innalzare il livello di protezione della mia privacy?

4.2.1 Sensibilizzare gli utenti sul tema del phishing

La sensibilizzazione degli utenti sul tema del phishing rappresenta un aspetto cruciale nella difesa contro gli attacchi informatici basati sull'ingegneria sociale. Questa forma di attacco mira a sfruttare la debolezza umana, ingannando le persone per ottenere informazioni sensibili o accesso non autorizzato a sistemi critici. Educare gli utenti su come riconoscere, prevenire e gestire tali minacce è fondamentale per proteggere non solo gli individui, ma anche le organizzazioni da conseguenze potenzialmente gravi[239].

Una delle prime strategie per sensibilizzare gli utenti riguarda la formazione e la

[239] CASSANO G., SCORZA G., VACIAGO G., *Diritto dell'internet,* Milano, 2012, p. 77 ss.

consapevolezza. È essenziale che le persone comprendano cosa sia il phishing, come funziona e quali sono le tattiche utilizzate dagli aggressori. Le sessioni di formazione dovrebbero includere esempi concreti di messaggi di phishing e insegnare agli utenti a individuarli. Questo è un punto di partenza fondamentale per costruire una solida difesa contro gli attacchi di phishing.

Inoltre, le organizzazioni possono condurre simulazioni di phishing controllate. Queste simulazioni permettono agli utenti di mettere in pratica le competenze apprese durante la formazione, testando la loro capacità di riconoscere e reagire correttamente a messaggi di phishing simulati. Questo approccio "hands-on" aiuta gli utenti a comprendere meglio le minacce ed a migliorare le loro abilità di difesa.

Le campagne di sensibilizzazione periodiche sono un altro strumento importante. Attraverso poster, email informative, webinar e altri mezzi di comunicazione interna, le organizzazioni possono mantenere alta l'attenzione degli utenti sulla minaccia del phishing. Queste campagne possono anche includere esempi reali di casi di phishing recenti, fornendo un contesto concreto e attuale.

Un aspetto critico della sensibilizzazione è l'incoraggiamento degli utenti a segnalare immediatamente qualsiasi sospetto di phishing ai team di sicurezza informatica. La tempestiva segnalazione è un elemento chiave nella prevenzione di potenziali attacchi e può contribuire a ridurre al minimo i danni.

Infine, mantenere gli utenti informati sugli sviluppi recenti nel mondo del phishing e sulle nuove tattiche utilizzate dagli aggressori è essenziale. Il phishing è un campo in continua evoluzione, e ciò che funzionava come truffa ieri potrebbe non funzionare oggi. Mantenere gli utenti al passo con le ultime tendenze è

fondamentale per garantire che siano pronti a riconoscere le nuove minacce[240].

In sintesi, la sensibilizzazione degli utenti sul phishing è un processo continuo che richiede l'impegno costante delle organizzazioni. Solo attraverso una solida comprensione del phishing e la pratica delle migliori pratiche di sicurezza informatica, gli utenti possono diventare un baluardo efficace contro questa minaccia in continua crescita.

4.2.2 L'impegno costante e l'apporto personale

L'impegno costante e l'apporto personale rivestono un ruolo centrale nella difesa contro le minacce informatiche, con particolare riferimento al fenomeno del phishing. Questi concetti, essenziali sia per gli utenti individuali che per le organizzazioni, rappresentano la linfa vitale della sicurezza informatica in un mondo sempre più connesso e vulnerabile.

L'impegno costante sottolinea l'importanza di un impegno duraturo nella promozione della sicurezza informatica. Ciò significa che la formazione e la consapevolezza sulla sicurezza non devono essere viste come eventi isolati o sporadici, ma come un processo in continuo divenire. Gli utenti dovrebbero partecipare regolarmente a programmi di formazione che tengano conto delle ultime minacce e delle migliori pratiche di difesa. La conoscenza è il primo passo per una difesa efficace, e mantenerla aggiornata è essenziale[241].

Un altro aspetto dell'impegno costante è l'adozione di una mentalità proattiva. Gli utenti dovrebbero essere attenti alle proprie attività online, monitorare gli account

[240] CASSANO G., SCORZA G., VACIAGO G., *Diritto dell'internet,* Milano, 2012, p. 99 s.

[241] CASSANO G., SCORZA G., VACIAGO G., *Diritto dell'internet,* Milano, 2012, p. 101.

e le transazioni in modo attivo e segnalare prontamente eventuali comportamenti sospetti. La sicurezza informatica richiede una partecipazione attiva da parte di ciascun individuo, che deve essere pronto a riconoscere, affrontare e segnalare potenziali minacce.

L'apporto personale è altrettanto cruciale. Implica il riconoscimento da parte di ciascun utente della propria responsabilità nella protezione dei dati personali e aziendali. Questo implica l'adozione di misure come la creazione di password robuste, la protezione adeguata dei dispositivi e la condivisione responsabile di informazioni. Ogni utente è un anello fondamentale nella catena di sicurezza informatica e il suo contributo personale ha un impatto diretto sulla resilienza complessiva contro le minacce.

Nelle organizzazioni, l'apporto personale significa che tutti i dipendenti devono essere coinvolti attivamente nella difesa contro il phishing e altre minacce. Questo coinvolge la collaborazione con i team di sicurezza informatica, la condivisione di informazioni pertinenti e la comunicazione aperta. L'adozione di procedure e politiche di sicurezza aziendale è un aspetto essenziale dell'apporto personale, poiché queste procedure rappresentano le linee guida per una pratica sicura e responsabile[242].

In conclusione, l'impegno costante e l'apporto personale sono i pilastri su cui si basa la difesa contro le minacce informatiche come il phishing. Attraverso la formazione continua, la vigilanza attiva e la collaborazione, sia gli utenti individuali che le organizzazioni possono rafforzare la propria resilienza alla crescente complessità delle minacce informatiche. La sicurezza informatica è un

[242] CASSANO G., SCORZA G., VACIAGO G., *Diritto dell'internet,* Milano, 2012, p. 103.

impegno collettivo che richiede la partecipazione e la consapevolezza di tutti.

4.2.3 Semplici consigli tecnici per proteggere la nostra riservatezza

La protezione della nostra privacy online è diventata una priorità in un'epoca in cui gran parte della nostra vita si svolge sul web. Ecco alcuni consigli pratici che possono aiutare chiunque a preservare la propria riservatezza online, senza richiedere una conoscenza tecnica avanzata.

Innanzitutto, è cruciale utilizzare password forti e uniche per ciascun account online. Queste password dovrebbero essere una combinazione di lettere maiuscole, minuscole, numeri e simboli, e non dovrebbero essere facili da indovinare. L'uso di gestori di password può semplificare notevolmente la gestione di password complesse[243].

Un altro passo importante è l'abilitazione dell'autenticazione a due fattori (2FA) ovunque sia possibile. Questo aggiunge un ulteriore strato di sicurezza richiedendo una verifica secondaria, come un codice inviato via SMS o un'app, oltre alla password.

Mantenere il software aggiornato è altrettanto essenziale. Questo non riguarda solo il sistema operativo, ma anche il software antivirus e tutte le applicazioni. Gli aggiornamenti spesso contengono correzioni di sicurezza vitali.

Le email di phishing rappresentano una delle minacce più comuni. Pertanto, è importante essere cauti quando si ricevono email da mittenti sconosciuti o

[243] CASSANO G., SCORZA G., VACIAGO G., *Diritto dell'internet,* Milano, 2012, p. 108.

sospetti. Non bisogna mai cliccare su link o scaricare allegati da queste email. Verificare attentamente l'indirizzo email del mittente prima di condividere informazioni o rispondere a messaggi è una pratica saggia.

Per la navigazione online, è consigliabile utilizzare connessioni HTTPS, riconoscibili dalla presenza di un lucchetto verde nell'URL. Questo indica che la connessione è cifrata, proteggendo le informazioni che inseriamo sui siti web.

La privacy sui social media è un'altra area di preoccupazione. Limitare le informazioni personali condivise sui social media e configurare le impostazioni di privacy in modo appropriato è fondamentale per evitare di esporre troppo la propria vita online[244].

L'uso di una Virtual Private Network (VPN) può contribuire a nascondere l'indirizzo IP e proteggere la propria privacy online. Questo è particolarmente utile quando si utilizzano reti Wi-Fi pubbliche non sicure.

Gestire i permessi delle app sui dispositivi è essenziale. Concedere solo i permessi necessari per il funzionamento dell'app può ridurre la quantità di dati a cui queste applicazioni possono accedere.

Infine, rimanere informati sulle ultime minacce online e partecipare a programmi di formazione sulla sicurezza informatica aiuta a mantenere una buona consapevolezza della sicurezza.

Seguire questi consigli tecnici può contribuire a preservare la nostra privacy online e proteggerci da molte delle minacce che possono mettere a rischio le nostre informazioni personali. La consapevolezza e l'adozione di buone pratiche

[244] CASSANO G., SCORZA G., VACIAGO G., *Diritto dell'internet,* Milano, 2012, p. 110.

sono fondamentali per una navigazione online sicura e responsabile[245].

Quanto poc'anzi analizzato è stato inserito personalmente in un sito web denominato www.phishingtips.it\home

[245] CASSANO G., SCORZA G., VACIAGO G., *Diritto dell'internet,* Milano, 2012, p. 111.

Phishing Tips

Che Cos'è:

È una particolare tipologia di truffa realizzata sulla rete internet attraverso l'inganno degli utenti convincendoli a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale. Attraverso un' email, solo apparentemente proveniente da istituti finanziari (banche o società emittenti di carte di credito) o da siti web che richiedono l'accesso previa registrazione. Il messaggio invita, riferendo problemi di registrazione o di altra natura, a fornire i propri riservati dati di accesso al servizio

Scopri Di Più

END-TO-END

Consigli Pratici

Solitamente nel messaggio per rassicurare falsamente l'utente è indicato un collegamento che rimanda solo apparentemente al sito web dell'istituto di credito o del servizio a cui si è registrato, in realtà il sito a cui ci si collega è stato allestito in modo identico a quello originale così che quando l'utente inserirà i propri dati riservati, questi saranno nella disponibilità dei criminali.

il sito a cui ci si collega è stato allestito in modo identico a quello originale così che quando l'utente inserirà i propri dati riservati, questi saranno nella disponibilità dei criminali.

1

Gli istituti di credito o le società che emettono carte di credito non chiedono mai la conferma di dati personali tramite email, ma contattano i propri clienti direttamente per tutte le operazioni riservate, perció diffidate dalle email che tramite un link in esse contenute, rimandano ad un sito web ove confermare i propri dati.
Nel caso riceviate una email, presumibilmente da parte della vostra banca, che vi fa richiesta dei dati personali riservati, recatevi personalmente presso il vostro istituto di credito.

Find Out More →

2

Se credete che l'email di richiesta informazione sia autentica, diffidate comunque del link presente in questa, collegatevi al sito della banca che l'ha inviata digitando l'indirizzo internet, a voi noti, direttamente nel browser.

Find Out More →

3

Verificate sempre che nei siti web dove bisogna immettere dati (account, password, numero di carta di credito, altri dati personali), la trasmissione degli stessi avvenga con protocollo cifrato.

4

Controllate, durante la navigazione in internet, che l'indirizzo URL sia quello del sito che si vuole visitare e non un sito "copia" creato per carpire dati
Nel caso riceviate una email, presumibilmente da parte della vostra banca, che vi fa richiesta dei dati personali riservati, recatevi personalmente presso il vostro istituto di credito.

Find Out More →

5

Installate sul vostro computer un filtro anti-spam

Find Out More →

Find Out More →

6

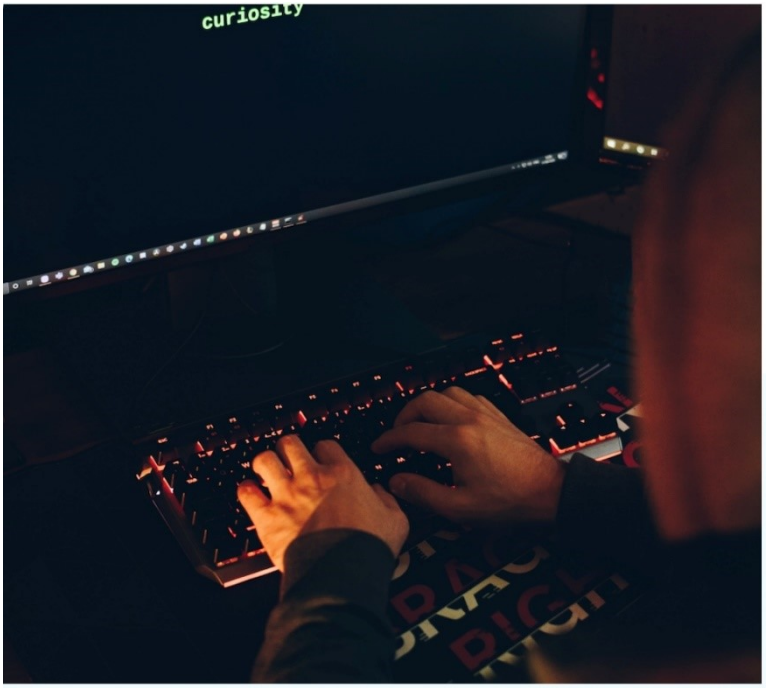
Controllate che, posizionando il puntatore del mouse sul link presente nell'email, in basso a sinistra del monitor del computer, appaia l'indirizzo internet del sito indicato e non uno diverso

Find Out More →

STRESS-FREE MOVING

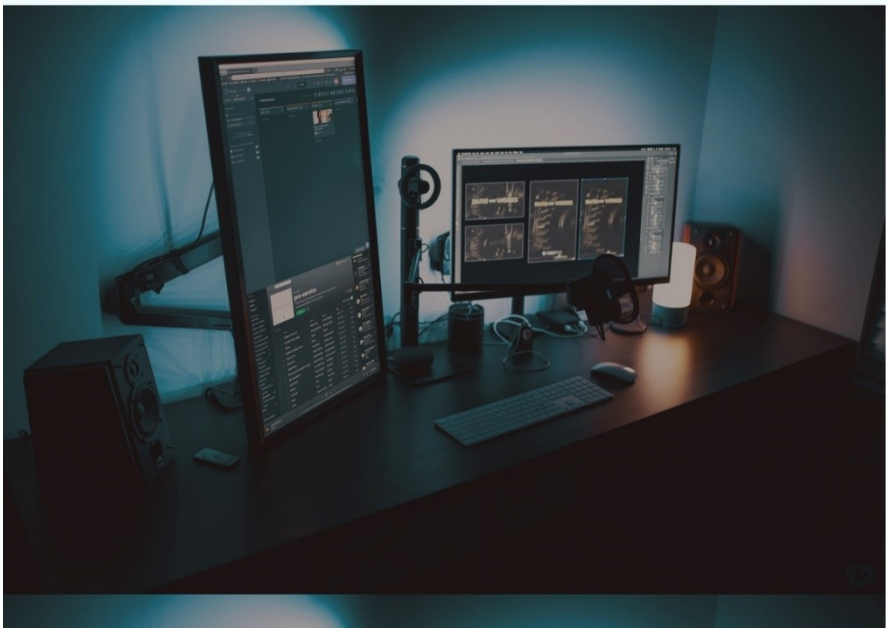
Consigli Pratici

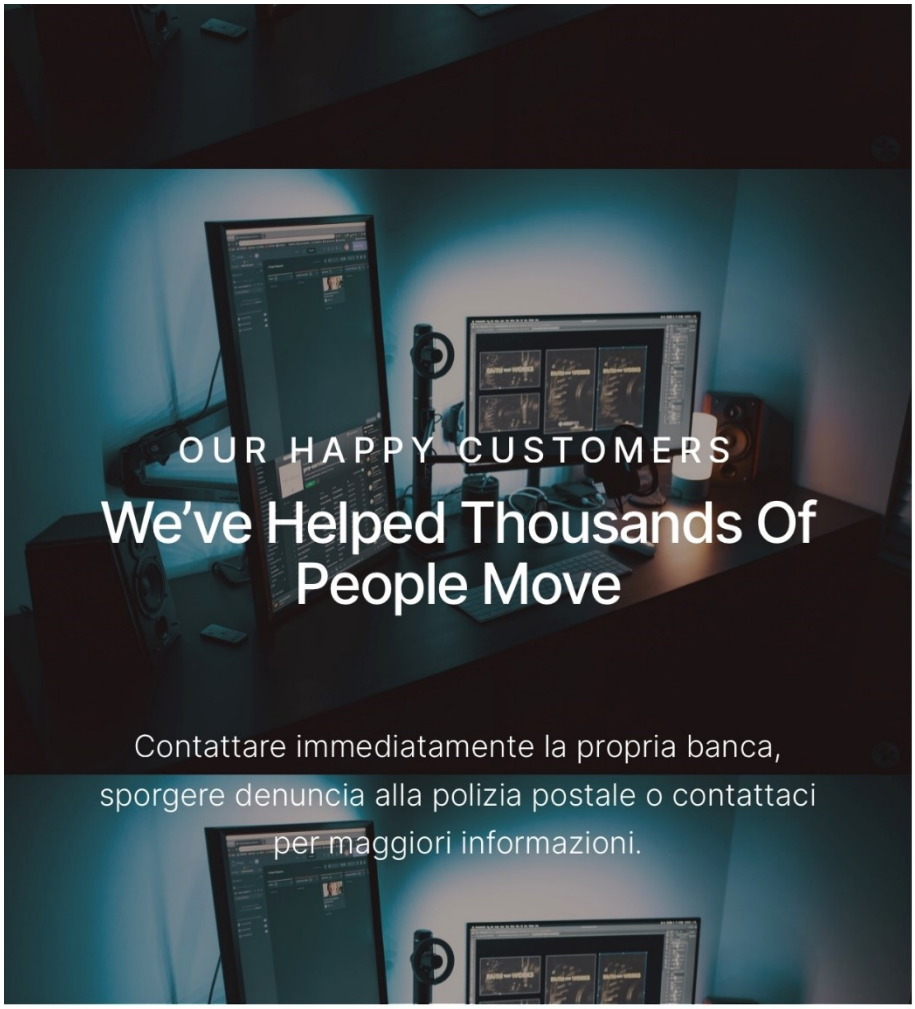
In generale il consiglio è di non comunicare mai i propri dati personali o bancari tramite il telefono o e-mail su richiesta di terzi.



GET EXCITED TO MOVE

The Process Is Easy!





+ 346 57 13994

4.3 Minori e internet

I nativi digitali sono le persone nate in un'epoca in cui la tecnologia digitale era già diffusa, essi non ricordano un tempo senza internet, e quindi hanno potuto apprenderne l'utilizzo sin dall'infanzia[246].

L'espressione è stata coniata da Marc Prensky, un educatore professionista che sostenne come i bambini esposti fin da subito all'uso della tecnologia digitale sviluppassero strutture d'apprendimento diverse rispetto a quelle della generazione immediatamente precedente, quella dei cosiddetti "migranti digitali" e che elaborassero persino le informazioni in maniera differente.

Sempre più fatti di cronaca ci fanno comprendere come l'utilizzo delle nuove tecnologie sia spesso, anche per i nativi digitali, un percorso denso di ostacoli e potenziali pericoli.

Gli adulti, che dovrebbero essere dei punti di riferimento nella formazione delle giovani generazioni, alle volte sottovalutano i "*percorsi cognitivi*" dei minori nella scoperta e nell'utilizzo degli strumenti del web 2.0.

Altre volte sono "impreparati" di fronte ad un universo, quello dei social network in particolare, in costante mutamento ed aggiornamento.

I social sono tanti e ogni anno si affacciano sul mercato nuovi "strumenti".

Pertanto, l'educazione digitale è centrale anche per i giovani, soprattutto i più piccoli, che devono imparare ad approcciarsi ad internet in maniera corretta.

È necessaria, quindi, un'attività di tipo didattico ed educativo finalizzata a sviluppare nei bambini la capacità di comprendere i diversi media e le varie

[246] Nativo digitale (voce) in Enciclopedia Treccani, www.treccani.it

tipologie di messaggi, utilizzarli correttamente, saper interpretare in maniera critica il messaggio ed essere in grado di generare un messaggio e quindi usare in maniera propositiva i media.

Tutte le recenti ricerche convergono sul fatto che sempre più persone (minori in particolare) accedono alla rete internet tramite cellulari, e questo rende ancora più importante l'educazione all'uso di internet.

Avere un account su Facebook, navigare in rete, usare un motore di ricerca come Google, vedere un video su Youtube, stare in chat mentre si gioca su una piattaforma online è spesso uno dei primi pensieri degli adolescenti ma anche dei bambini spesso abituati a cercare su Youtube i video dei loro cartoni preferiti.

Il Web viene fruito dai minori sempre più tramite dispositivi mobili che aumentano la portata e la possibilità di navigare sulla rete in occasioni diverse ed alle volte, fuori dal controllo di un adulto.

Senza contare che occorre monitorare e preservare anche la loro reputazione online perché magari compiono azioni che, per la loro età, può sembrare normale ma che magari potrebbe causare danni di immagini nel loro futuro[247].

Anche in questo senso l'educazione svolge una funzione essenziale, che non serva reprimere ma formare e la scuola dovrebbe essere all'avanguardia nelle competenze e nelle conoscenze dei nuovi strumenti digitali.

[247] Prova dell'importanza della web reputation è data dal fatto che tutt'oggi, alla luce dei numerosi fatti di cronaca, si parla e si propongono disegni di leggi in materia di diritto all'oblio e reputazione digitale,

4.4 Anziani e truffe: linee guida dettagliate per rilevare e proteggersi dai tentativi di phishing

Vista la poca dimestichezza con internet e con gli strumenti intelligenti gli anziani sono tra le vittime più diffuse di phishing.

Gli anziani sono dunque oggetto di spam (messaggi di posta elettronica non richiesti di carattere pubblicitario, in alcuni casi anche in forma aggressiva), che possono arrivare a infestare la casella e-mail.

In alcuni casi i messaggi contengono 'inviti' minacciosi ad acquistare certi prodotti che non garantiscono assolutamente né qualità né certificazione, ma nella gran parte delle circostanze lo spam sconfina nel phishing.

Per questo da anni la Polizia di Stato e le altre Forze dell'Ordine propongono campagne di informazione e prevenzione.

Nel 2023, con lo slogan" *Anziani più informati, anziani più sicuri*", la campagna nazionale contro le truffe agli anziani "più sicuri insieme", promossa dall'Associazione nazionale anziani e pensionati di Confartigianato (Anap) insieme al Ministero dell'Interno, e nello specifico la Direzione centrale della polizia criminale del Dipartimento della pubblica sicurezza, ha raggiunto la quinta edizione[248].

Secondo i dati della Polizia di Stato "*il 50% degli anziani sono vittime di truffe online e l'altra metà di truffe tradizionali*", aggiungendo che "*inizia ad esserci un'alfabetizzazione digitale tale per cui gli over 65 accedono al mondo digitale e*

[248] FRANZELLA N. G., Più sicuri insieme contro le truffe agli anziani, 18 aprile 2023, www.poliziadistato.it

talvolta ne rimangono anche vittime, al pari della popolazione under 65. La fascia di età più colpita è quella tra i 65 e i 70 anni. Fino agli 80 anni i maschi sono più vittime delle donne, quasi il doppio nella fascia 65-70: a fronte di 3049 donne abbiamo 5712 maschi[249]*."*

Per questo si rende necessario prestare la massima attenzione al fenomeno e prevenire questi odiosi reati attraverso il contributo delle forze di Polizia in un'azione comune per difendere i cittadini, soprattutto in vista dei mesi estivi durante i quali si moltiplicano i rischi per gli anziani che rimangono soli e più esposti al rischio truffe.

La Polizia di Stato è parte attiva della campagna informativa, che si prefigge di organizzare su tutto il territorio nazionale convegni ed incontri, per mettere in guardia gli anziani sui pericoli delle truffe più ricorrenti e, così facendo, aiutarli a difendersi. Inoltre, è prevista la distribuzione in tutta Italia di vademecum e dépliant che contengono poche semplici regole, suggerite dalle forze di polizia, per difendersi dai rischi di truffe, raggiri, furti e rapine in casa, per strada, sui mezzi di trasporto, nei luoghi pubblici, ma anche utilizzando Internet[250].

[249] Discorso Prefetto Dott. Rizzi alla presentazione della V edizione di "Più sicuri insieme", 18 aprile 2023, www.poliziadistato.it

[250] CASSANO G., SCORZA G., VACIAGO G., *Diritto dell'internet,* Milano, 2012, p. 133.

4.5 Le prospettive future e gli sviluppi previsti nel campo del phishing

Il phishing è un problema persistente e in continua evoluzione nel campo della sicurezza informatica. Le prospettive future sulle sfide e gli sviluppi nel campo del phishing includono nuove tecniche di attacco, misure di prevenzione emergenti e soluzioni innovative.

Il "Deepfake Phishing" è una minaccia emergente nell'ambito della sicurezza informatica che si basa sull'uso di tecnologie avanzate di manipolazione multimediale, note come "deepfake", per ingannare le vittime. Queste tecnologie consentono di creare contenuti audio e video falsificati che sembrano straordinariamente autentici, con personaggi o figure di fiducia che sembrano parlare o agire in modo credibile. Questo crea un terreno fertile per gli attacchi di phishing, in cui gli aggressori possono impersonare individui noti o figure di autorità per indurre le vittime a compiere azioni dannose o a condividere informazioni sensibili[251].

Il processo di un attacco di Deepfake Phishing di solito inizia con la selezione di un bersaglio, seguito dalla creazione di un deepfake su misura. Gli aggressori raccolgono informazioni sul bersaglio per personalizzare il messaggio, rendendolo ancora più convincente. Una volta creato il deepfake, viene distribuito alla vittima attraverso canali come e-mail o messaggi di testo. La vittima, vedendo o ascoltando il messaggio, potrebbe essere convinta che provenga da una fonte

[251] A. Leonardi, *Deepfake Phishing, cos'è e come contrastare i rischi*, in https://www.cybersecurity360.it/nuove-minacce/deepfake-phishing-cose-e-come-contrastare-i-rischi/, 2023.

di fiducia e potrebbe essere indotta a compiere azioni dannose o a rivelare dati riservati.

Per proteggersi da questo tipo di attacco, è essenziale adottare una serie di misure preventive. La formazione e l'educazione delle persone sono fondamentali, poiché aiutano le vittime a riconoscere segnali di deepfake e comportamenti sospetti. Inoltre, è importante verificare sempre l'identità delle persone prima di seguire istruzioni o condividere informazioni sensibili basate su messaggi audio o video. L'uso di strumenti di rilevamento avanzati per identificare deepfake e l'implementazione di politiche di sicurezza rigorose per la gestione delle comunicazioni e l'accesso ai dati sono anch'essi cruciali[252].

In conclusione, il Deepfake Phishing è una minaccia crescente che sfrutta le tecnologie di manipolazione multimediale per trarre in inganno le vittime. Affrontare questa minaccia richiede una combinazione di sensibilizzazione, formazione e misure tecnologiche avanzate per garantire la sicurezza digitale contro questi attacchi sempre più sofisticati.

Ancora, l'uso dell'Intelligenza Artificiale nel phishing rappresenta un passo avanti nella strategia degli hacker per ingannare le persone e le organizzazioni. Con l'AI, gli aggressori possono personalizzare in modo estremamente accurato i loro attacchi, rendendoli incredibilmente convincenti. Sotto il profilo pratico, l'AI può raccogliere una vasta quantità di dati su potenziali vittime, dai loro comportamenti online alle loro preferenze personali. Questi dati vengono quindi utilizzati per creare messaggi di phishing altamente personalizzati, che sembrano provenire da fonti di fiducia o corrispondere agli interessi delle vittime. Questa

[252] A. Leonardi, *Deepfake Phishing, cos'è e come contrastare i rischi*, cit.

personalizzazione rende le truffe incredibilmente difficili da rilevare[253].

Ma l'AI non si ferma qui. Può anche generare automaticamente i contenuti di phishing, scrivendo e-mail o messaggi di testo con un linguaggio naturale che sembra autentico. Questo non solo semplifica il lavoro degli hacker, ma rende anche più difficile per i sistemi di sicurezza tradizionali rilevare questi messaggi come minacce.

Un altro aspetto interessante è l'automazione del processo di attacco. L'AI può gestire tutto il processo, dalla creazione dei messaggi alla loro distribuzione. Ciò significa che gli aggressori possono lanciare una vasta campagna di phishing in modo rapido ed efficiente, aumentando le probabilità di successo.

Inoltre, l'AI può imparare dai comportamenti delle vittime nel tempo, adattando gli attacchi in base a nuove informazioni raccolte. Questo significa che gli attacchi possono diventare sempre più mirati e convincenti man mano che l'AI accumula dati.

Per difendersi da questo tipo di minaccia, è essenziale adottare una serie di misure preventive. Le organizzazioni devono investire in soluzioni di rilevamento avanzate che utilizzano l'AI e il machine learning per identificare schemi sospetti nelle comunicazioni. Allo stesso tempo, la formazione delle persone è fondamentale per insegnare loro a riconoscere gli indicatori di phishing, anche quando gli attacchi sono altamente personalizzati[254].

Inoltre, l'adozione di autenticazione a due fattori (2FA) può rendere più difficile per gli aggressori l'accesso non autorizzato, anche se riescono a ottenere le

[253] A. Leonardi, *Deepfake Phishing, cos'è e come contrastare i rischi*, cit.

[254] CASSANO G., SCORZA G., VACIAGO G., *Diritto dell'internet,* Milano, 2012, p. 151.

credenziali di accesso tramite un attacco di phishing. La collaborazione tra aziende e la condivisione delle informazioni sugli attacchi di phishing possono aiutare a identificare le minacce in modo più rapido ed efficace[255].

Come si può reagire? Esistono soluzioni innovative in tal senso? La blockchain offre alcune potenziali soluzioni per prevenire il phishing, sebbene non possa risolvere completamente il problema da sola. La blockchain può essere utilizzata per creare sistemi di autenticazione decentralizzati basati su chiavi crittografiche. Invece di affidarsi a un'unica autorità centrale per verificare l'identità degli utenti, una blockchain può essere utilizzata per convalidare le identità in modo distribuito. Gli utenti possono avere le loro chiavi private sicure su una blockchain, rendendo più difficile per gli aggressori falsificarle.

Le firme digitali basate su blockchain possono essere utilizzate per convalidare la provenienza delle comunicazioni. Ad esempio, quando si riceve un'e-mail o un messaggio con una firma digitale basata su blockchain, è possibile verificarne l'autenticità attraverso la blockchain stessa, riducendo così il rischio di phishing[256].

Gli NFT basati su blockchain possono essere utilizzati per autenticare documenti, contratti o comunicazioni importanti. Se una persona riceve un documento firmato come NFT, può verificarne l'autenticità consultando la blockchain.

La caratteristica principale della blockchain è la sua immutabilità. Questo significa che una volta che i dati sono registrati su una blockchain, non possono essere modificati o cancellati senza il consenso della maggioranza della rete. Questo

[255] G.J. Sicignano, *Bitcoin e riciclaggio*, Torino, 2019, p. 18 s.

[256] CASSANO G., SCORZA G., VACIAGO G., *Diritto dell'internet,* Milano, 2012, p. 161.

può essere utilizzato per creare registri immutabili di comunicazioni legittime, consentendo alle persone di verificare facilmente se una comunicazione è stata alterata[257].

Gli smart contract basati su blockchain possono essere utilizzati per automatizzare il processo di verifica delle comunicazioni. Ad esempio, uno smart contract potrebbe essere programmato per verificare automaticamente l'autenticità di un'e-mail o di un messaggio in base a criteri specifici registrati sulla blockchain.

Tuttavia, è importante notare che la blockchain da sola non è una panacea per il phishing. Gli attacchi di phishing coinvolgono spesso l'ingegneria sociale e la manipolazione psicologica delle vittime, quindi anche se le comunicazioni sono verificate sulla blockchain, le persone potrebbero ancora essere ingannate. Inoltre, l'adozione su larga scala di soluzioni basate su blockchain richiederebbe un impegno significativo e potrebbe comportare sfide tecniche e regolamentari[258].

In definitiva, la blockchain può essere un elemento utile nella prevenzione del phishing, ma dovrebbe essere utilizzata in combinazione con altre misure di sicurezza, tra cui l'istruzione delle persone e l'uso di tecniche di riconoscimento delle truffe.

[257] G.J. Sicignano, *Bitcoin e riciclaggio*, cit., p. 80.

[258] CASSANO G., SCORZA G., VACIAGO G., *Diritto dell'internet,* Milano, 2012, p. 171.

4.5.1 Informatizzazione e innovazione

L'informatizzazione e l'innovazione rappresentano un aspetto fondamentale nella lotta contro il phishing, un tipo di minaccia informatica che continua a evolversi in termini di sofisticazione e diffusione. La capacità di sfruttare le tecnologie avanzate è essenziale per sviluppare e implementare soluzioni sempre più efficaci per proteggere sia gli individui che le organizzazioni da questo tipo di attacchi.

Uno dei progressi più significativi è il rilevamento automatico del phishing. Qui entrano in gioco algoritmi di machine learning e intelligenza artificiale che possono identificare schemi comuni nelle email di phishing. Questi algoritmi sono addestrati per riconoscere automaticamente email sospette e bloccarle prima che raggiungano la casella di posta dell'utente. Questo approccio basato sui dati permette una maggiore precisione nella rilevazione e una risposta più rapida alle minacce[259].

Le soluzioni di filtraggio delle email stanno diventando sempre più sofisticate grazie all'apprendimento automatico. Questi filtri possono analizzare il contenuto e i metadati delle email per individuare segnali di phishing, aiutando a prevenire l'apertura di messaggi dannosi.

L'autenticazione a due fattori (2FA) è un altro ambito in cui l'innovazione ha un ruolo chiave. Le soluzioni di 2FA possono essere integrate in modo più agevole nei processi di accesso online, ad esempio mediante l'uso di app mobili per generare codici di autenticazione. Questo rende molto più difficile per gli

[259] CASSANO G., SCORZA G., VACIAGO G., *Diritto dell'internet,* Milano, 2012, p. 151.

aggressori superare questa barriera di sicurezza.

I browser web moderni sono dotati di funzionalità avanzate di sicurezza per proteggere gli utenti dal phishing. Queste funzioni possono includere l'indicazione della sicurezza dei siti web, il rilevamento di siti contraffatti e la segnalazione di siti sospetti. Ciò consente agli utenti di navigare in modo più sicuro online.

L'educazione sulla sicurezza informatica sta diventando sempre più interattiva, con l'uso di simulazioni di phishing che permettono agli utenti di sperimentare situazioni di phishing in modo sicuro e apprendere come riconoscerle.

L'analisi del comportamento degli utenti rappresenta un ulteriore livello di protezione. Le soluzioni di sicurezza possono monitorare le attività online degli utenti per individuare comportamenti anomali, come l'invio di dati sensibili a destinatari non abituali, e attivare un avviso in caso di potenziale minaccia[260].

In sintesi, l'informatizzazione e l'innovazione sono centrali nella difesa contro il phishing. Continuando a sfruttare le tecnologie avanzate, possiamo sviluppare soluzioni sempre più efficaci per prevenire, rilevare e mitigare gli attacchi di phishing, contribuendo a mantenere un ambiente digitale più sicuro per tutti. La sfida continua è quella di rimanere un passo avanti agli aggressori, sfruttando al meglio le risorse tecnologiche a nostra disposizione.

[260] CASSANO G., SCORZA G., VACIAGO G., *Diritto dell'internet,* Milano, 2012, p. 172.

4.5.2 Nuove tecniche di attacco e misure di prevenzione emergenti

L'evoluzione delle minacce informatiche è un tema di grande rilevanza nella sicurezza informatica contemporanea. Gli aggressori, spesso sofisticati e altamente motivati, sviluppano costantemente nuove tecniche di attacco per superare le difese digitali. Questa dinamica ha portato alla necessità di sviluppare misure di prevenzione altrettanto avanzate per proteggere dati e sistemi.

Una delle tendenze più significative è rappresentata dalle nuove tecniche di ingegneria sociale. Gli aggressori cercano sempre più di manipolare le emozioni e le convinzioni delle persone per ottenere informazioni sensibili o accesso non autorizzato a sistemi. Questi attacchi, spesso mirati e personalizzati, sfidano la capacità delle persone di riconoscerli[261].

Inoltre, il ransomware ha subito un'evoluzione con la tattica della "double extortion," in cui i criminali non si limitano a cifrare i dati, ma minacciano anche di rivelare tali dati pubblicamente se non viene pagato un riscatto. Questo comporta conseguenze significative per le vittime, aumentando la pressione per adottare misure di protezione efficaci.

Altre minacce emergenti includono l'exploit delle vulnerabilità zero-day, che sfruttano falle sconosciute nei sistemi, e il phishing basato sull'intelligenza artificiale, che genera messaggi di phishing altamente convincenti e difficili da distinguere da comunicazioni legittime.

Per contrastare queste minacce, gli esperti di sicurezza stanno adottando una

[261] CASSANO G., SCORZA G., VACIAGO G., *Diritto dell'internet,* Milano, 2012, p. 175.

serie di misure di prevenzione avanzate. L'analisi comportamentale sta diventando uno strumento chiave per rilevare attività anomale e rispondere prontamente. Le soluzioni di sicurezza avanzate, come i sistemi SIEM (Security Information and Event Management), utilizzano l'apprendimento automatico e l'analisi del contesto per identificare minacce in tempo reale.

L'automazione è sempre più importante per rispondere rapidamente agli attacchi, in quanto consente di avviare azioni correttive senza ritardi dovuti all'intervento umano. La difesa in profondità rimane una strategia chiave, che coinvolge l'uso di molteplici strati di sicurezza per proteggere l'intera infrastruttura[262].

Inoltre, l'educazione continua degli utenti è essenziale per aiutare le persone a riconoscere le nuove minacce emergenti. La consapevolezza degli utenti è spesso l'anello più debole nella catena di sicurezza, ma una formazione continua può contribuire a rafforzare questo aspetto critico.

Infine, l'adozione di architetture di sicurezza Zero Trust, che presume che nulla sia attendibile e richiede l'autenticazione continua e rigorosa, rappresenta un cambiamento significativo nell'approccio alla sicurezza.

In sintesi, mentre le minacce informatiche continuano a evolversi, la comunità della sicurezza informatica sta rispondendo con misure altrettanto avanzate e innovative. La sfida rimane quella di rimanere un passo avanti rispetto agli aggressori, sfruttando al meglio le tecnologie e le pratiche emergenti per proteggere dati e sistemi digitali[263].

[262] CASSANO G., SCORZA G., VACIAGO G., *Diritto dell'internet,* Milano, 2012, p. 177.

[263] CASSANO G., SCORZA G., VACIAGO G., *Diritto dell'internet,* Milano, 2012, p. 179.

4.5.3 Policy antiphishing

Le politiche antiphishing costituiscono un fondamentale pilastro della strategia di sicurezza informatica all'interno di qualsiasi organizzazione. Questi documenti delineano in modo chiaro e dettagliato le linee guida e le procedure da seguire per proteggersi dagli attacchi di phishing, una delle minacce più diffuse e insidiose nell'ambiente digitale odierno.

Innanzitutto, è essenziale che tali politiche definiscano in modo preciso cosa si intende per phishing, spiegando che si tratta di una pratica malevola mediante la quale gli aggressori cercano di ingannare le persone al fine di ottenere informazioni sensibili o accesso non autorizzato a sistemi o dati. Questa definizione fornisce una base solida per la comprensione della minaccia da parte di tutti gli attori coinvolti.

Un altro elemento cruciale nelle politiche antiphishing è l'attribuzione di responsabilità. Chi è responsabile dell'implementazione delle misure antiphishing? Questo dovrebbe essere chiaramente definito, dal personale di sicurezza informatica alle squadre di gestione, fino agli utenti finali. Ognuno deve conoscere il proprio ruolo e le proprie responsabilità nella prevenzione e nella gestione degli attacchi di phishing.

La formazione e la sensibilizzazione degli utenti rappresentano una parte fondamentale di queste politiche. Gli utenti devono essere informati su come riconoscere le comunicazioni sospette, come comportarsi in caso di sospetto phishing e quali procedure seguire in caso di incidente. La consapevolezza degli utenti è un fattore cruciale nella prevenzione degli attacchi di phishing, e le politiche dovrebbero sottolineare l'importanza di un impegno continuo in questo

senso.

Un altro elemento chiave è l'uso dell'autenticazione a due fattori (2FA). Questa misura aggiuntiva di sicurezza, che richiede una verifica oltre alla password, dovrebbe essere incoraggiata e implementata ovunque sia possibile[264].

Le politiche antiphishing dovrebbero anche delineare requisiti rigidi per la creazione e la gestione delle password, promuovendo l'uso di password complesse e la loro regolare modifica. Inoltre, dovrebbero stabilire l'obbligo di utilizzare filtri anti-phishing per rilevare e bloccare email sospette prima che raggiungano gli utenti.

Un'altra componente importante riguarda le procedure di risposta agli incidenti. Le politiche dovrebbero dettagliare come gestire gli attacchi di phishing, incluse le azioni da intraprendere in caso di sospetto o conferma di un attacco. La prontezza nella risposta può fare la differenza nel mitigare i danni causati da un attacco di phishing.

Infine, la condivisione delle informazioni tra organizzazioni è sempre più cruciale. Le politiche dovrebbero promuovere questa pratica, in modo che dati e indicatori di compromissione possano essere scambiati tra diverse entità per migliorare la capacità di risposta collettiva alle minacce emergenti.

In conclusione, le politiche antiphishing costituiscono un documento fondamentale per qualsiasi organizzazione che desidera proteggersi dalle insidie del phishing. Queste politiche devono essere chiare, comunicate in modo efficace e soggette a revisione regolare per affrontare le nuove minacce che emergono costantemente nel mondo digitale. La sicurezza informatica è una sfida in

[264] CASSANO G., SCORZA G., VACIAGO G., *Diritto dell'internet,* Milano, 2012, p. 179.

costante evoluzione, e le politiche antiphishing svolgono un ruolo chiave nella difesa degli asset digitali.

CAPITOLO V
Rilievi conclusivi

5.1 L’utilizzo abituale e quotidiano di strumenti tecnologici

Alla luce delle considerazioni svolte nel presente elaborato, si può giungere ad interessanti conclusioni in merito al fenomeno dei *cybercrime.*

Non vi è dubbio che, al giorno d'oggi, la quasi totalità delle attività sociali, lavorative e ludiche si svolgono sempre più mediante l'utilizzo di strumenti tecnologici ed informatici.

Ciò ha determinato l'aumento delle possibilità di crescita per la società, poiché l'*e-commerce,* l'*home banking* e il *trading on-line* rendono sempre più efficienti e celeri gli scambi e le comunicazioni.

D'altro canto, tale informatizzazione ha determinato l'aumento delle possibilità di commissione dei c.d. reati informatici.

5.2 I cybercrimes: una minaccia reale e concreta

Difatti, i *cybercrimes* rappresentano ormai una minaccia concreta per la società contemporanea, al pari di qualunque altro tipo di reato. L'utilizzo quotidiano dei *computers* è diffuso non solo tra i giovani ma anche tra gli anziani, spesso senza avere la consapevolezza dei rischi connessi a tale uso, esponendosi agli attacchi di altri utenti, sicuramente più scaltri, i quali fanno leva sull'ingenuità e l'inesperienza altrui.

La vulnerabilità degli utenti di fronte ai *phishing attacks* è sempre più evidente, soprattutto in un periodo storico come quello attuale ove, a causa dell'emergenza sanitaria dovuta alla diffusione del virus COVID-19, si è intensificato l'utilizzo delle

strumentazioni informatiche al fine di far fronte alle necessità quotidiane, le quali non possono più essere concretamente soddisfatte in altro modo, in un contesto di continuo (purtroppo!) *lockdown*.

5.3 Richiesta di un'adeguata forma di tutela

Di fronte a tale costante utilizzo delle tecnologie nella vita di ogni giorno, sarebbe opportuno, se non necessario, che l'ordinamento giuridico italiano predisponga un apparato normativo incisivo, che sia in grado di tutelare dagli attacchi informatici, intervenendo tempestivamente con misure adeguate, qualora vengano scoperti i primi segnali di violazioni alle barriere di protezione.

Difatti, giunge ormai da più parti la richiesta di una normativa *ad hoc* che sia in grado di rispettare e valorizzare la libertà di utilizzo dei dispositivi informatici e delle reti telematiche e, al contempo, di tutelare nel miglior modo possibile le vittime dei reati informatici.

Affinché tale obiettivo venga raggiunto, sarebbe utile, da una parte, una maggiore campagna di sensibilizzazione ed informazione, tale da fornire agli utenti un'utile conoscenza dei rischi a cui si sottopongono mediante l'utilizzo della strumentazione informatica e, dall'altra, l'inserimento di un nuovo complesso di reati nel codice penale, prevedendo un inasprimento del trattamento sanzionatorio, al fine di scoraggiare i *phishers* dal compimento delle condotte criminose.

5.3.1 La campagna di sensibilizzazione per le fasce della popolazione più a rischio

Una sicura conclusione cui si può arrivare all'esito dell'analisi compiuta è che le vittime statisticamente più colpite dal phishing sono gli anziani.

Vista la poca dimestichezza con internet e con gli strumenti intelligenti gli anziani sono tra le vittime più diffuse di phishing.

Gli anziani sono dunque oggetto di spam (messaggi di posta elettronica non richiesti di carattere pubblicitario, in alcuni casi anche in forma aggressiva), che possono arrivare a infestare la casella e-mail.

In alcuni casi i messaggi contengono 'inviti' minacciosi ad acquistare certi prodotti che non garantiscono assolutamente né qualità né certificazione, ma nella gran parte delle circostanze lo spam sconfina nel phishing.

Per questo da anni la Polizia di Stato e le altre Forze dell'Ordine propongono campagne di informazione e prevenzione.

Nel 2023, con lo slogan" *Anziani più informati, anziani più sicuri*", la campagna nazionale contro le truffe agli anziani "più sicuri insieme", promossa dall'Associazione nazionale anziani e pensionati di Confartigianato (Anap) insieme al Ministero dell'Interno, e nello specifico la Direzione centrale della polizia criminale del Dipartimento della pubblica sicurezza, ha raggiunto la quinta edizione[265].

Secondo i dati della Polizia di Stato "*il 50% degli anziani sono vittime di truffe online e l'altra metà di truffe tradizionali*", aggiungendo che "*inizia ad esserci*

[265] FRANZELLA N. G., Più sicuri insieme contro le truffe agli anziani, 18 aprile 2023, www.poliziadistato.it

un'alfabetizzazione digitale tale per cui gli over 65 accedono al mondo digitale e talvolta ne rimangono anche vittime, al pari della popolazione under 65. La fascia di età più colpita è quella tra i 65 e i 70 anni. Fino agli 80 anni i maschi sono più vittime delle donne, quasi il doppio nella fascia 65-70: a fronte di 3049 donne abbiamo 5712 maschi[266]*."*

Inoltre, la polizia postale, in collaborazione con l'Associazione Bancaria Italiana (ABI) e Poste Italiane, ha dato avvio ad un'attività di sensibilizzazione degli utenti la quale, mediante gli istituti bancari, vengono avvisati del pericolo rappresentato dal fenomeno del *phishing*.

Dal punto di vista della repressione di tale condotta illecita, la polizia postale ha avviato quasi 1.200 indagini di propria iniziativa nonché altre 900 su richiesta dell'autorità giudiziaria: gli interventi in questioni hanno consentito di denunciare circa 80 persone nonché di procedere a perquisizioni. Ne è derivato che la maggior parte delle minacce proveniva da Paesi dell'Europa orientale.

5.4 Analisi delle varie fasi del phishing al fine di comprendere quale norma attuare concretamente

Poiché, come si è già anticipato, il legislatore non si è ancora occupato di dettare una disciplina specifica per i *phishing attacks*, al fine di comprendere quale delle norme attuali si possano concretamente applicare ai singoli casi di specie, occorre ben considerare ogni fase in cui l'attacco può suddividersi.

[266] Discorso Prefetto Dott. Rizzi alla presentazione della V edizione di "Più sicuri insieme", 18 aprile 2023, www.poliziadistato.it

Ed invero, in tal senso si distingue una prima fase, consistente nell'invio di un messaggio *e-mail* avente ad oggetto un *link* di rinvio alla pagina *web* non autentica, finalizzato a spingere l'utente a rivelare proprie informazioni personali riservate. La seconda fase consiste nella “raccolta” dei dati riservati dell'utente attraverso tale sito oppure mediante un *form* da compilare con le informazioni personali richieste. Infine, nella terza fase vi è l'utilizzo delle informazioni raccolte al fine di accedere ai servizi *on-line* o alle aree riservate in maniera abusiva, oppure allo scopo di utilizzare in maniera indebita carte di credito o di pagamento, realizzando un profitto.

I social sono tanti e ogni anno si affacciano sul mercato nuovi “strumenti”.

Pertanto, l’educazione digitale è centrale anche per i giovani, soprattutto i più piccoli, che devono imparare ad approcciarsi ad internet in maniera corretta.

5.4.1 Attività didattica di educazione per i minori

È necessaria, quindi, un’attività di tipo didattico ed educativo finalizzata a sviluppare nei bambini la capacità di comprendere i diversi media e le varie tipologie di messaggi, utilizzarli correttamente, saper interpretare in maniera critica il messaggio ed essere in grado di generare un messaggio e quindi usare in maniera propositiva i media.

Tutte le recenti ricerche convergono sul fatto che sempre più persone (minori in particolare) accedono alla rete internet tramite cellulari, e questo rende ancora più importante l’educazione all’uso di internet.

Avere un account su Facebook, navigare in rete, usare un motore di ricerca come Google, vedere un video su Youtube, stare in chat mentre si gioca su una

piattaforma online è spesso uno dei primi pensieri degli adolescenti ma anche dei bambini spesso abituati a cercare su Youtube i video dei loro cartoni preferiti.
Il Web viene fruito dai minori sempre più tramite dispositivi mobili che aumentano la portata e la possibilità di navigare sulla rete in occasioni diverse ed alle volte, fuori dal controllo di un adulto.
Senza contare che occorre monitorare e preservare anche la loro reputazione online perché magari compiono azioni che, per la loro età, può sembrare normale ma che magari potrebbe causare danni di immagini nel loro futuro.

5.5 Le norme penali che vengono in essere nel caso di specie

In definitiva, l'attività di *phishing* può ricondursi alla fattispecie di truffa di cui all'art. 640 c.p., tutte le volte in cui il *phisher,* ponendo in essere artifici e raggiri determinati dalla sostituzione di persona – realizzata mediante la creazione ed utilizzazione di un falso *account* di posta elettronica attribuibile ad un apparente vero e diverso soggetto – dopo aver indotto in errore la vittima ed essersi fatto rivelare i codici di accesso, si introduce nel suo servizio di *home-banking*, compiendo degli atti dispositivi determinanti un impoverimento del patrimonio della vittima, con pari profitto in proprio favore.
L'elemento oggettivo del reato si identifica con la condotta del soggetto agente, il quale induce in errore la persona offesa, millantando di essere la propria banca di fiducia o una nota società di *e-commerce,* inducendo la vittima a comunicare i propri dati riservati.

In seguito, il soggetto indotto in errore realizza l'atto di disposizione patrimoniale, il quale è causa dell'ingiusto profitto con altrui danno.

D'altronde, l'appropriazione fraudolenta di codici e *password* non è altro che lo strumento attraverso il quale il *phisher* è in grado di ottenere, mediante gli artifici e i raggiri tipici di tale fenomeno illecito, l'indebito profitto patrimoniale, realizzando in tal modo la condotta e l'evento propri della truffa.

Riferimenti

Bibliografici

AGNINO F., *Computer crime e fattispecie penali tradizionali: quando il phishing integra il delitto di truffa*, in *Il Corriere del Merito*, 3, 2009.

ALAGNA I.M., *Il giurista informatico: "Digital Single Market" e approccio olistico*, in *Ciberspazio e diritto*, 2, 2017.

ALMA M., PERRONI C., *Riflessioni sull'attuazione delle norme a tutela dei sistemi informatici*, in *Diritto penale processuale*, 1997.

AMATO MANGIAMELI A.C., SARACENI G., *I reati informatici: elementi di teoria generale e principali figure criminose*, Milano, 2015.

AMORE S., STANCA V., STARO S., *I crimini informatici. Dottrina, giurisprudenza ed aspetti tecnici delle investigazioni,* Massa Carrara, 2006.

ARONICA G., *Il "fishing" tra nuove esigenze di tutela ed acrobazie interpretative della giurisprudenza*, in *Il Foro ambrosiano*, 1, 2008.

ASTROLOGO C., *Prime riflessioni sulla definizione di reato transnazionale nella Legge n. 146/2006,* in *Cass. Pen.,* 2007

BATTELLI E., *Contrattazione e condizioni generali di contratto nell' e-commerce*, in *I contr.*, n. 2, 2010.

BERGHELLA F., BLAIOTTA R., *Diritto penale dell'informatica e beni giuridici*, in *Cassazione penale*, 1995.

BONAVITA S., CORTINA A., STRINGHI E., "*Conosci il tuo nemico": un primo approccio tassonomico ai principali attacchi informatici nel settore "cybercrime" bancario e finanziario*, in *Ciberspazio e Diritto*, 3, 2020.

BRENNER S., *Defining Cybercrime: a review of Federal and State Law,* in CLIFFORD R.D., *Cybercrime,* 2018

BRIAT M., SIEBER U., *Computer Related Criminality Analysis of Legal Policy in the OECD Area,* Parigi, 1986

BUFFA F., *Profili penali del commercio elettronico*, Milano, 2006.

BUTTARELLI G., *Le sfide del "Big Data" tra evoluzione tecnologica, etica e interessi collettivi*, in *Gnosis*, 2, 2017.

CADOPPI A., CANESTRARI S., PAPA M., MANNA A., *Trattato di diritto penale parte speciale*, Milano, 2013

CAJANI F., *Profili penali del phishing*, in *C.P.,* 2007

CAJANI F., *La tutela penale dell'identità digitale alla luce delle novità introdotte dal d.l. 14 agosto 2013, n. 93 (convertito con modificazioni dalla l. 15 ottobre 2013, n. 119)*, in *Cassazione penale*, 3, 2014.

CAJANI F., COSTABILE G., MAZZARACO G., *Phishing e furto di identità digitale. Indagini informatiche e sicurezza bancaria,* Milano, 2008.

CAMPBELL D., *Il mondo sotto sorveglianza. Ekelon e lo spionaggio globale elettronico globale*, Feltrinelli, Milano, 2003.

CASSANO G., *Diritto delle nuove tecnologie informatiche e dell'internet,* Milano,

2002

CASSANO G., SCORZA G., VACIAGO G., *Diritto dell'internet,* Milano, 2012.

CICCONE A., *La sfida del terrorismo ai media e ai social network*, in *www.valigiablu.it*, 18 luglio 2017.

CIPOLLA P.M., *E-commerce e truffa,* in *Giur di mer.,* n. 12, Milano, 2013.

CONTRAFFATTO V., *I reati informatici*, Milano, 2015.

CORASANITI G., *La tutela della comunicazione informatica e telematica,* in BORRUSO, BUONOMO, CORASANITI, D'AIETTI (a cura di), *Profili penali dell'informatica*, Milano, 1994.

CIPOLLA P., *"Social network", furto di identità e reati contro il patrimonio*, in *Giurisprudenza di merito*, 12, 2012.

CRESCIOLI C., *Le diverse fasi dei "phishing attacks": le fattispecie vigenti e i problemi applicativi in prospettiva comparata tra Italia e Germania* in *L'Indice penale*, 3, 2021.

CURTOTTI D., *Procedimento penale e 'intelligence' in Italia: un'osmosi inevitabile, ancora orfana di regole*, in *Processo penale e Giustizia*, 3, 2018.

D'AIUTO G., LEVITA L., *I reati informatici. Disciplina sostanziale e questioni processuali*, Milano, 2012.

DI LELLA F., *Utilizzo fraudolento di credenziali informatiche nei servizi di "home banking" e responsabilità civile dell'istituto di credito*, in *Il Foro napoletano*, 1, 2015.

DI LEMBO V., *La disciplina del "phishing"*, in *Rivista penale*, 9, 2013.

DI LEMBO V., *Il "phishing": dall'illecita captazione di dati alla truffa*, in *Rassegna dell'Arma dei Carabinieri*, 4, 2013.

DI LEMBO V., *La frode informatica*, in *Rivista penale*, 4, 2013.

DI STASIO C., *La lotta multilivello al terrorismo internazionale. Garanzia di sicurezza versus tutela dei diritti fondamentali*, Milano, 2010.

DORE G., *I doveri di informazione nella rete degli scambi commerciali telematici*, in *Giur. di mer*., Milano, 2013, n. 12.

FAINI F., PIETROPAOLO S., *Scienza giuridica e tecnologie informatiche*, Torino, 2017.

FANELLI A., *Commento all'art. 640 c.p.,* in LATTANZI-LUPO, *Codice penale, Rassegna di giurisprudenza e di dottrina,* Milano, 2005.

FANTINI M., *Phishing: strategie operative dell'inganno*, in Diritto dell'Internet, 4, 2008.

FEROLA L., *Il riciclaggio da phishing: tra vecchie e nuove questioni interpretative*, in *Giurisprudenza di merito*, 11, 2009.

FIANDACA G., MUSCO E., *Diritto penale. Parte speciale*. *I reati contro il patrimonio*, Bologna, 2012.

FINOCCHIARO G., DELFINI F., *Diritto dell'informatica,* Milano, 2014.

FIORIGLIO G., *Sorveglianza e controllo nella società dell'informazione. il possibile contributo dell'etica hacker*, in *Nomos. Le attualità del diritto.*

Quadrimestrale di teoria generale, diritto pubblico comparato e storia costituzionale 2, 2014.

FLOR R., *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. online-Durchsuchung*, in *Riv. trim. dir. pen. ec.*, 2009

FLOR F., *Phishing, identify theft e identify abuse: le prospettive applicative del diritto penale vigente,* in *RIDPP,* 2007

FLOR R., *Tutela penale e autotutela tecnologica dei diritti d'autore nell'epoca di Internt,* Padova, 2010.

FLOR R., *Phishing e profili penali dell'attività illecita di "intermediazione" del c.d. financial manager*, in *Diritto penale e processo*, 1, 2012.

FLOR R., *Lotta alla criminalità informatica e tutela di tradizionali e nuovi diritti fondamentali nell'era di Internet,* in *Diritto Penale Contemporaneo,* 20 settembre 2012

FOLLIERI L., *Il contratto concluso via internet,* Napoli, 2005.

FRAU R., *"Home banking", captazione di credenziali di accesso dei clienti tramite "phishing" e responsabilità della banca*, in *Responsabilità civile e previdenza*, 3, 2015.

GALLI L.C., *"Intelligence" e "Data Science". Un binomio possibile?*, in *Gnosis*, 2, 2017.

GIACONA I., *Istanze europee di "ne bis in idem" e posizioni attuali della dottrina italiana sul concorso apparente dei reati*, in *Diritto penale e processo*, 3, 2022.

GIORDANO M.T., VACIAGO G., *La qualificazione giuridica del Phishing in una delle sue applicazioni giurisprudenziali*, in *Diritto dell'Internet*, 1, 2007.

IMBESI A.G., *Phishing and pharming on the net*, in *Il Nuovo Diritto*, 7-8, 2006.

IZZI S., *Intelligence e gestione delle informazioni. Attività preventiva contro i traffici illeciti*, Milano, 2011.

LAMANUZZI M., *Accesso abusivo ad un sistema informatico o telematico: prospettive di riforma*, in *Archivio penale*, 1, 2022.

MALGIERI L., *La nuova fattispecie di indebito utilizzo di identità digitale: un problema interpretativo,* in *Dir. Pen. Cont.,* 2015

MANTOVANI F., *Diritto penale, Parte speciale*, II, *Delitti contro il patrimonio*, Padova, 2002.

MENDUNI E., *I media digitali. Tecnologie, linguaggi, usi sociali*, Bari, 2014.

MERLI A., *Il diritto penale dell'informatica: legislazione vigente e prospettive di riforma*, in *Giustizia penale*, 2, 1993.

MODESTI G., *Il reato di frode informatica. Una rilettura alla luce delle recenti traiettorie giurisprudenziali*, in *Ragiusan*, 335-337, 2012.

MORGANTE G., *Il reato come elemento del reato. Analisi e classificazione del concetto di reato richiamato dalla fattispecie penale,* Torino, 2018.

MOSCA C., *I servizi di informazione e il segreto di Stato (legge 3 agosto 2007, n. 124)*, Milano, 2008.

MUGAVERO R., *Armi non convenzionali, nuovi scenari della sicurezza e "Cbrne*

intelligence", in *Gnosis* 2, 2015.

PARODI C., *Profili penali dei virus informatici*, in *Diritto penale processuale*, 2000.

PAZIENZA F., *In tema di criminalità informatica: l'art. 4 della legge 23 dicembre 1993, n. 547*, in *Rivista di diritto penale processuale*, 1995.

PECORELLA C., *Il diritto penale dell'informatica*, Padova, 2006.

PERRI P., *Lo smishing e il vishing, ovvero quando l'unico limite all'utilizzo criminale delle nuove tecnologie è la fantasia*, in *Diritto dell'Internet*, 3, 2008.

PERRI P., *Analisi informatico-giuridica delle più recenti interpretazioni giurisprudenziali in tema di phishing*, in *Ciberspazio e Diritto*, 1, 2008.

PERRI R., *Lo smishing e il vishing, ovvero quando l'unico limite all'utilizzo criminale delle nuove tecnologie è la fantasia,* in *Diritto dell'Internet,* 2008

PICOTTI L., *Biens juridiques protégés et techniques de formulation des incriminations en droit pénal de l'informatique,* in *Rev. Int. Droit pénal*, 2006.

PICOTTI L., *Commento art. 5 L. 23.12.1993, n. 547 (art. 616, comma 4, c.p.),* in *Leg. Pen.,* 1996

PICOTTI L., *Ratifica della Convenzione Cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo*, in *Dir. dell'Internet*, 5, 2008.

PICOTTI L., *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale,* in *Dir. Pen. Proc.,* 2008, n. 6.

PICOTTI L., *I diritti fondamentali nell'uso e abuso dei social network. Aspetti penali,* in *Giur. Merito,* n. 12, 2012.

PICOTTI L., *Sicurezza informatica e diritto penale,* in DONINI, PAVARINI, *Sicurezza e diritto penale,* Bologna, 2011

PICOTTI L., *La nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee,* in *Riv. Trim. dir. Pen. ec.,* 2011.
PITINO S., *L'intelligence e l'analisi di contrasto al crimine organizzato*, Roma, 2006.

PITTARO, *Indebito utilizzo di una carta di credito e truffa: concorso di reati o concorso apparente?,* in *Dir. Pen. Proc.,* 1995.

PRESSACO L., *Intelligenza artificiale e ragionamento probatorio nel processo penale*, in *BioLaw Journal - Rivista di BioDiritto*, 4, 2022.

ROMANO B.N., *Il rischio di "attacchi" ai sistemi informatici tra fattispecie penalmente rilevanti, tutela dei dati ed esigenze di "buona amministrazione"* in Amministrativ@mente, 3, 2021.

RUSSO B., *I nuovi orientamenti giurisprudenziali sul reato di "phishing": "La banca è responsabile se non prova che il cliente ha disposto il pagamento"*, in *Rivista di diritto bancario*, 4, 2019.

SARZANA DI S. IPPOLITO, *Informatica, internet e diritto penale*, Milano, 2010.

SCOPINARO L, *Internet e i reati contro il patrimonio,* collana diretta da G. Fiandaca, E. Musco, T. Padovani, F. Palazzo, Torino, 2007

SERICOLA E., *Cybercrime e diritti fondamentali nell'era di Internet,* in *Filodiritto*, 9 maggio 2017,

STAZI A., *Commercio elettronico ed utilità delle informazioni da fornire ai clienti*,

in *Dir. dell'inf*., 2009.

VALSECCHI A., *Brevi osservazioni di diritto penale sostanziale*, in *Diritto penale processuale*, 2005.

VERRI A., *Contenuto ed effetti (attuali e futuri) della direttiva 2011/93/UE,* in *Dir. Pen. Cont.,* 28 marzo 2012.

ZANASI A., *Nuove forme di guerra, nuove forme di intelligence: Text Mining. Intelligence in XXI Century*, Roma, 2001.

ZICCARDI G., *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Milano, 2015.

Giurisprudenza

Di legittimità

Cass. Pen., 4 ottobre 1999, n. 3067
Cass. Pen. 4 ottobre 1999, n. 214945
Cass. Pen. 1 ottobre 2004, n. 2672
Cass Pen. 8 marzo 2006, n. 2225
Cass Pen. 8 novembre 2007, n. 46674
Cass. Pen. 24 febbraio 2011, n. 9891
Cass Pen. 24 novembre 2003, n. 33656
Cass. Pen. 15 dicembre 2019, n. 12479
Cass. Pen. 2 dicembre 2022, n.6395
Cass. Pen. 28 ottobre 2022, n.2682

Di merito

GIP, Trib. Milano, sent. 10 dicembre 2007

Trib. Milano, sent. 7 ottobre 2001, n. 11696

Trib. Nola, sent. 11 dicembre 2007

Trib. Milano, 19 marzo 2007

Tribunale Milano, 07 ottobre 2011

Trib. Parma, sent. 6 settembre 2018, n. 1268

Trib. Arezzo, sent. 8 aprile 2020, n. 272

Giudice di Pace di Treviso, sent. 16 settembre 2021, n. 963

Normativa

Europea

Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica, 23 novembre 2001

Proposta di direttiva del Parlamento europeo del Consiglio COM (2010) 517 – C7 - 0293/2010 – 2010/0273(COD)

Decisione quadro 2004/68/GAI del Consiglio, del 13 dicembre 2011

Comunicazione della Commissione al Consiglio e al Parlamento europeo del 28 marzo 2012

Nazionale

Legge n. 633/41

Legge n. 197/1991

Legge n. 547/1993

Dlg. n. 231/2001

D.lgs n. 196/2003

Legge n. 146/2006

Legge n. 48/2008

Legge n. 93/2013

Legge n. 119/2013

Sitografia

MASSA R.G., *Il phishing,* 2008, reperibile sul sito *http://www.pmi.it/impresa/normativa/articolo/1999/il-phishing.html*

SAMBUCCI L., *Falsi call center sul VoIP: la nuova truffa si chiama Vishing,* in *www.anti-phishing.it* , 2006.

SURACE C., *Dal Phishing al Vishing*: *l'evoluzione della truffa come conseguenza dell'evoluzione tecnologica,* (a cura di), Ricerca svolta presso l'Osservatorio CSIG (Centro Studi Informatica Giuridica) di Reggio Calabria, in www.filodiritto.com, 2007