DIPARTIMENTO DI GIURISPRUDENZA

CATTEDRA DI DIRITTO PENALE 2

LE TRUFFE *ON-LINE*

RELATORE

Chiar.mo Prof.

Antonino Gullo

CANDIDATA

Giulia Cioeta
Matr. 141393

CORRELATORE

Chiar.mo Prof.

Enrico Gallucci

ANNO ACCADEMICO 2019/2020

INDICE

INTRODUZIONE

Il progresso tecnologico e le nuove forme di connessione fra sistemi informatici e telematici hanno determinato un importante impatto sulla società moderna, comportando permanenti mutamenti nelle dinamiche sociali e relazionali.

Lo sviluppo delle nuove tecnologie ha certamente provocato l'insorgenza di innumerevoli vantaggi individuali e collettivi con riferimento a qualsiasi contesto. Gli effetti dirompenti della digitalizzazione, quale massima espressione di cambiamento, hanno influenzato, pertanto, interi settori della società, e in particolare il diritto, la cui evoluzione ha fortemente risentito della suddetta rivoluzione informatica.

La formazione di una nuova e indefinita dimensione, indicata con il termine "*cyberspace*", offre agli individui molteplici e inedite opportunità di diversa natura. Essa è connotata da dematerializzazione, aterritorialità e atemporalità, quali segni distintivi di una realtà totalmente distante da quella fisica e materiale che si è abituati ad affrontare.

Tuttavia, al di là degli intuitivi aspetti positivi propri della digitalizzazione, si individuano non poche criticità riconducibili ad insidiose e originali forme di aggressione, capaci di pregiudicare numerosi beni giuridici. A tal proposito, si deve considerare la difformità di valore esistente tra le condotte materiali, realizzate nella realtà fisica, e le condotte digitali, poste in essere nell'ambiente cibernetico, vale a dire quei comportamenti perpetrati in rete mediante l'impiego degli strumenti telematici a disposizione.

Il dominio cibernetico, dunque, rappresenta un terreno fertile per la criminalità, e tra i settori in cui questa si è maggiormente manifestata e rafforzata vi è quello delle c.d. "truffe *on-line*", espressione utilizzata per indicare una categoria generale all'interno della quale è possibile individuare diverse tipologie di reato.

Alla luce di ciò, il presente elaborato si prefigge l'obiettivo di esaminare i profili penali relativi alle truffe commesse in rete, al fine di identificare le analogie e le differenze esistenti tra la fattispecie di truffa perpetrata a mezzo *web* e quella di frode informatica, nonché i rapporti tra queste e le altre figure delittuose

abitualmente commesse nel cyberspazio. Il lavoro, dunque, propone una lettura lungimirante ed estensiva del delitto di truffa comune, volta ad estendere l'applicabilità della norma in esame nei casi in cui tale crimine sia posto in essere nel contesto digitale, tentando di adattarla alle tipicità proprie del *cyberspace.*

Ulteriore scopo perseguito per mezzo della presente trattazione è quello di inquadrare penalmente, nell'ambito delle truffe *on-line*, il complesso fenomeno fraudolento di *social engineering*, denominato *phishing*, a fronte della continua evoluzione del *modus operandi* che lo contraddistingue e della difficoltà di individuare la fattispecie entro cui esso è sussumibile.

Inoltre, la trattazione rileva la comparsa di nuove esigenze di protezione, sottolineando la necessità di ridefinire la tutela penale degli interessi patrimoniali degli utenti, in virtù degli elementi distintivi della realtà tecnologica, e di elaborare risposte concrete alle problematiche poste da questa nuova forma di criminalità.

Si sente, dunque, il bisogno di condurre un'indagine di natura giuridica su una realtà completamente nuova, e sulle numerose modalità di realizzazione dei fenomeni fraudolenti che in essa si manifestano.

Nel dettaglio, l'elaborato si articola in tre capitoli, nel tentativo di svolgere un'analisi confacente alle criticità inerenti alle truffe commesse *on-line*, in virtù della loro pericolosità e della preoccupazione sociale che da esse deriva.

Il primo capitolo è volto a fornire un quadro generale di riferimento, al fine di contestualizzare le truffe digitali, partendo *in primis* dall'esposizione dell'evoluzione delle nuove tecnologie e dell'impatto che queste hanno avuto sui rapporti giuridici e sociali, per poi passare ad un'analisi più dettagliata del cyberspazio, quale nuova dimensione difficilmente identificabile e sprovvista di confini spazio-temporali, scenario prediletto per porre in essere minacce e *cyberattacks*, i quali saranno oggetto di successiva esposizione.

Nel prosieguo si volgerà lo sguardo all'evoluzione normativa in tema di reati cibernetici, evidenziando le loro peculiarità ed il passaggio dai *computer crimes* ai *cybercrimes*, nonché l'inversione di rotta del legislatore, il quale, al fine di contrastare la criminalità informatica e di rendere il cyberspazio un luogo sicuro, ha prediletto l'adozione di misure preventive a quelle repressive, favorendo la nascita della *cybersecurity*.

Il secondo capitolo entrerà nel cuore del presente lavoro, ovverosia le truffe *on-line*, soffermando l'attenzione, in particolare, sui reati di truffa e di frode informatica, dei quali si propone una dettagliata analisi dei profili di ordine sostanziale, nonché delle relative difficoltà applicative in ragione del peculiare contesto di riferimento.

Si affronterà in via introduttiva la tutela del patrimonio nel cyberspazio, considerando le diverse concezioni del bene giuridico che sono state condivise nel corso del tempo dalla dottrina, e successivamente l'attenzione si focalizzerà sui rapporti tra le suddette fattispecie e le altre figure *criminis* che trovano nel cyberspazio un "non-luogo" di realizzazione, evidenziando volta per volta le posizioni dottrinali e giurisprudenziali in merito.

Di seguito si discuterà delle truffe commesse in danno dei consumatori digitali, nel particolare ambito delle piattaforme *e-commerce* e degli *on-line criminal markets.*

Saranno poi oggetto di analisi i problemi giuridici relativi all'individuazione del *locus commissi delicti* nelle truffe *on-line*; a tal proposito verranno prospettate le questioni attinenti al momento consumativo dei reati in esame, riportando l'orientamento condiviso dalle Sezioni Unite della Cassazione, che, come si vedrà, ha condotto a risultati di diverso tipo, sulla base del differente metodo di pagamento utilizzato dal soggetto passivo.

Infine, nel terzo capitolo si approfondirà il fenomeno del *phishing*, quale complessa tecnica di attacco finalizzata a capire fraudolentemente i dati riservati degli utenti; a questo riguardo si analizzeranno le diverse fasi di cui esso si compone, tentando, al contempo, di inquadrarlo dal punto di vista normativo, non essendo prevista una disciplina giuridica *ad hoc*, e affrontando, a seconda dei casi, le criticità inerenti alla sussistenza e alla possibile coesistenza di precise norme giuridiche, tra le quali, appunto, la truffa commessa a mezzo *web* e la frode informatica.

Si disquisirà poi sull'evoluzione del suddetto fenomeno e delle sue numerose ed innovative forme di manifestazione, concludendo con l'esame del caso di *smishing* "CartaSì" – quale concreto esempio di attacco cibernetico perpetrato mediante l'invio di *sms* – e tenendo conto altresì delle critiche relative alla

configurabilità dei delitti e all'effettiva applicabilità delle norme individuate dal giudice competente per il caso.

CAPITOLO I

IL CYBERSPAZIO: I CONFINI DELLA SICUREZZA CIBERNETICA

1.1 Lo sviluppo delle nuove tecnologie e l'impatto sui rapporti giuridici e sociali.

La rapida evoluzione delle nuove tecnologie informatiche e telematiche[1] ha interessato interi settori della società moderna ed ha totalmente rivoluzionato molteplici aspetti della vita di ciascun individuo[2].

Le *ICT*, infatti, consentono di elaborare, comunicare, memorizzare e divulgare informazioni, mediante strumenti digitali, in modo semplice e veloce, ed il loro sviluppo ha consentito l'accesso e l'utilizzo di tali mezzi a chiunque, dapprima limitato a una ristretta cerchia di professionisti.

I mutamenti connessi alle *ICT* hanno avuto un così rilevante impatto sulle condizioni sociali ed individuali da influenzare l'applicazione del diritto vigente, non solo penale, e da interessare l'operato di legislatori nazionali e di organismi internazionali che, seppur in momenti differenti e in virtù di distinte esigenze, nonché di diverse condizioni politiche, culturali e tecnologiche, sono intervenuti sulla regolazione del fenomeno.

In ragione della rilevanza giuridica della suddetta innovazione e, in particolare, dell'importanza che questa assume per il diritto penale, anche la dottrina e la giurisprudenza hanno cominciato a confrontarsi con l'argomento a partire dagli ultimi decenni della seconda metà del XX secolo, seppur, inizialmente, alcuni settori più tradizionalisti della dottrina penale si erano mostrati scettici circa il rilievo di questo nuovo campo del diritto. Tuttavia, al giorno d'oggi, è opinione condivisa quella che riconosce il valore, l'autonomia e l'attualità della materia, la

[1] Cfr. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in CADOPPI, CANESTRARI, MANNA, PAPA (diretto da), Cybercrime, Torino, 2019, 35.: con tale espressione "tecnologie informatiche e telematiche" «si deve intendere l'ampia nozione, corrente nella terminologia internazionale, di nuove "tecnologie dell'informazione e della comunicazione": c.d. T.I.C o, in inglese, *I.C.T* (*Information and Communication Technologies*)».

[2] Cfr. SIRILLI, v*oce Innovazione tecnologica, in Enc. della scienza e della tecnica*, 2008, reperibile su *www.treccani.it*: «L'innovazione tecnologica non è un fatto meramente tencnico-scientifico, ma un processo sociale di natura dinamica».

quale è meritevole, peraltro, di un'opportuna elaborazione teorica e sistematica, nonché di appropriate analisi ermeneutiche.

Inoltre, sarebbe opportuno considerare il tema alla luce di un approccio nuovo ed esteso, volto alla revisione dell'intero sistema penale, e giuridico in generale, favorendo l'interconnessione tra il progresso tecnologico, il diritto e i rapporti sociali, e sottolineando anche le relative conseguenze sulla teoria generale del diritto e del reato.

L'evoluzione del diritto, quindi, ha fortemente risentito della c.d. "rivoluzione informatica o cibernetica", poiché in una società globalizzata e moderna come quella attuale questo tipo di sviluppo rappresenta, ed ha rappresentato, senz'altro, la massima espressione di cambiamento, capace, appunto, di produrre effetti sociali, politici, culturali e, di conseguenza, economici e giuridici.

L' uso del termine " rivoluzione" è indicativo proprio del fatto che l' evento informatico travolge ogni aspetto della vita privata e collettiva, non solo con riguardo alla semplificazione e alla rapidità delle modalità di informazione e comunicazione, rese possibili in qualunque luogo e momento ad opera di chiunque, ma anche con riferimento al concreto svolgimento delle quotidiane attività pubbliche e private in molteplici ambiti, tanto da poter individuare con esattezza una linea di confine tra "il prima" e "il dopo" la rivoluzione informatica.

I potenziali effetti di tale innovazione cibernetica sul diritto sono innumerevoli e non ancora esauriti e, a tal proposito, volendone citare alcuni immediatamente riscontrabili, di rilievo centrale nell'ambito del dibattito scientifico, non si può non considerare l'intelligenza artificiale, la robotica e il processo telematico come esempi di nuove frontiere del diritto.

La rivoluzione cibernetica ha determinato, inoltre, la nascita di nuovi interessi, bisognosi di tutela giuridica, e, di conseguenza, di nuovi diritti da affiancare a quelli tradizionali.

Sono state altresì facilitate nuove forme di aggregazione e partecipazione, in virtù delle molteplici e nuove possibilità di ritrovo, che hanno favorito la condivisione di obiettivi e valori comuni in una dimensione del tutto inedita.

Accogliendo, per completezza espositiva, una prospettiva di studio più ampia e generalizzata, al di là dell'ambito più strettamente penalistico, è

indispensabile evidenziare che il connubio tra il diritto e le nuove tecnologie informatiche e telematiche ha determinato la contemporanea genesi di due diversi settori di ricerca e approfondimento: «da una parte l' informatica giuridica e cioè quella scienza che studia come le nuove tecnologie possano essere utilizzate dagli operatori del diritto per meglio svolgere la propria attività; dall' altra il diritto dell'informatica e cioè quella disciplina che si occupa dei problemi giuridici sollevati dall'uso delle nuove tecnologie nella nostra società e quindi delle norme che regolano le tecnologie dell'informazione e della comunicazione nella c.d. "*information society*", poiché è l'informatica a costituire oggetto dello studio e dell'approfondimento del diritto »[3].

Senza voler anticipare quanto si approfondirà in seguito, a proposito del quadro normativo relativo al diritto penale dell'informatica, si ritiene doveroso sottolineare, già da ora, lo stretto collegamento tra le fonti del diritto dell'informatica e l'espansione tecnologica nel nostro Paese, in ragione di una parallela e costante evoluzione.

A tal proposito sono, convenzionalmente, distinguibili tre fasi, non sulla base di specifici riferimenti temporali, ma rispetto alle peculiarità delle fonti del diritto dell'informatica ad essi connesse. La prima, in cui si evidenzia il passaggio dall'informatica accentrata, per pochi, a quella distribuita, per tutti, grazie alla nascita dei *personal computer*; fase, questa, contraddistinta da fonti a carattere principalmente giurisprudenziale e in cui si ravvisano inadeguati e sporadici tentativi di produzione delle prime norme del diritto dell'informatica. La seconda, nella quale emerge una sempre maggiore diffusione dell'informatica, non più relegata esclusivamente all'ambito lavorativo, ma estesa anche a quello domestico, e la nascita della telematica e delle sue prime applicazioni. È in questa seconda fase che si assiste ad un più intenso sviluppo normativo, avente ad oggetto la sovrapposizione tra diritto e tecnologia, per la gran parte di derivazione comunitaria, finalizzato a stabilire regole comuni all'interno della c.d. "società dell'informazione"[4].

---

[3] Cfr. CIACCI, *L' ordinamento giuridico e le fonti del diritto dell'informatica*, in VALENTINO (a cura di), *Manuale di diritto dell'Informatic*a, Napoli, 2011, 7.

[4] Cfr. SIRILLI, voce *Società dell'informazione, in Enc. della scienza e della tecnica*, 2008, *www.treccani.it*: «La società dell'informazione è un contesto in cui le nuove tecnologie informatiche

Infine, la terza, seguente all'avvento della rete Internet, che ha condotto all'esponenziale divulgazione delle nuove tecnologie ed alla nascita di innovative ed estese modalità informative e comunicative, tra le quali i c.d. "social networks", con conseguente diffusione di problematiche giuridiche nuove e diverse rispetto alle precedenti fasi.

Nel primo periodo, definito "pionieristico", era stata messa in dubbio la reale possibilità di identificare un diritto dell'informatica, poiché non esistevano, a quel tempo, né un'adeguata disciplina specifica, né una comune regolazione della materia, ma, al contrario, si registrava un uso eccessivo dell'estensione applicativa degli istituti di diritto comune a questioni piuttosto settoriali, aventi ad oggetto attività svolte mediante strumenti informatici e telematici.

È dunque nel corso di un successivo momento, detto di "consolidamento", che si individua la concreta produzione di norme nel diritto dell'informatica. La manifestazione della c.d. "società dell'informazione", nell'ambito di questa seconda fase di progresso della materia, è giustificata dalla sempre maggiore affermazione delle tecnologie sviluppatesi in prima fase[5].

Gli aspetti imprescindibili della suddetta società tecnologica sono rappresentati dall'informatica e dalla telematica, intese, congiuntamente, come motore di crescita sociale, il cui ulteriore progresso è avvenuto con la comparsa della rete Internet, nella terza fase, che ha esteso ancor di più la portata dei concetti di informazione e comunicazione, attribuendogli un significato sociale e giuridico di maggiore profondità e rilevanza. Proprio l'avvento della rete Internet ha indotto ad interrogarsi sulla validità e sull'efficienza delle norme precedentemente emanate; lo stesso ha avuto, inoltre, ulteriori effetti immediatamente riscontrabili nella proliferazione di fonti normative volte a disciplinare le nuove attività, anche di

---

e di telecomunicazione assumono un ruolo fondamentale nello sviluppo delle attività umane. Queste tecnologie servono a produrre e comunicare, in forma digitale, messaggi, immagini, testi, musica, filmati, e così via».

[5] V. CIACCI, *L' ordinamento giuridico e le fonti del diritto dell'informatica*, cit., 14 s.: «La c.d. società dell'informazione, come concetto e come programma politico, viene definita inizialmente nel c.d. Rapporto Bangemann del 1994, che affronta i diversi aspetti di tale società e redige un programma di interventi comunitari al fine di una sua espansione e affermazione. Con riferimento alle tecnologie dell'informazione, si registra in seguito a tale importante documento l'emanazione di diverse direttive, le prime delle quali strettamente collegate allo sviluppo del mercato dell'informazione in rete. Successivamente vengono disciplinati gli aspetti collegati ad alcune materie più prettamente di diritto dell'informatica[…]».

natura autoregolamentare, e nell'aumento della produzione giurisprudenziale. Quanto suddetto si è dimostrato funzionale al proseguimento dell'opera di realizzazione della società dell'informazione antecedentemente intrapresa.

Sulla base delle considerazioni sin qui elaborate, emerge che le fonti del diritto dell'informatica nascono in una determinata realtà tecnologica e trovano applicazione in quella stessa realtà che però, essendo soggetta ad uno sviluppo rapido e costante, esige pronte risposte normative alle relative problematiche da essa derivanti.

Tuttavia, da sempre, tale più veloce mutamento della tecnologia dei sistemi informatici e telematici, volto a soddisfare un'esigenza sociale di innovazione, si è mal conciliato con i classici strumenti di produzione del diritto; infatti, spesso l'autoregolamentazione ha anticipato la tradizionale produzione legislativa, e frequentemente la giurisprudenza, nella sua funzione suppletiva e integrativa, è stata chiamata a fronteggiare le immediate difficoltà del caso concreto.

Pertanto, è ulteriormente deducibile che, in questo settore, all'incessante novità tecnica non corrisponde una altrettanto rapida regolamentazione giuridica, in virtù della sopraindicata maggiore celerità con la quale la tecnologia si evolve rispetto alla produzione normativa, ragion per cui si deve dare atto di un ritardo nell'affrontare i relativi problemi e dell'esistenza di numerose fonti di natura eterogenea, e non necessariamente normative, del diritto dell'informatica.

In altri termini, quindi, l'indiscutibile reciprocità di condizionamento fra realtà cibernetica e diritto richiede un continuo e necessario adeguamento di quest'ultimo, affinché possa estendere la propria attività regolatrice anche ai nuovi fenomeni poc'anzi indicati, impiegando tutti gli strumenti di cui dispone, tra i quali indubbiamente la creazione di nuove norme e il ricorso all'interpretazione evolutiva e all'applicazione analogica, seppur inevitabilmente camuffata nell'ambito penale[6].

[6] Cfr. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, cit., 40 s.: «[…]Come ogni realtà strutturale che condiziona le sovrastrutture, la rivoluzione cibernetica modifica e ridetermina il suo stesso rapporto con il diritto, toccandone le funzioni e il modo di operare, per taluno ponendo a rischio proprio il suo nucleo essenziale, se non l'esistenza, in quanto la tecnologia sembra in grado di porsi in concorrenza o conflitto con la sua primaria funzione normativa: il "codice tecnico" si presenta con la pretesa di essere il nuovo codice giuridico– "*Code is Law*", per citare il famoso libro di Lawrence Lessig – l'autotutela tecnologica e l'autoregolazione dei signori del *web* tende a divenire diritto od a sostituirlo, perché realmente ed immediatamente si applica od "autoapplica", configurando in tempo reale nuovi precetti muniti di relative ed efficaci

Si rilevano, in virtù del particolare e diretto collegamento alla rete Internet, la vocazione internazionale e la natura interdisciplinare, quali caratteristiche ulteriori delle citate fonti e delle questioni ad esse connesse.

L'automazione dei processi di elaborazione dei dati, che avviene per mezzo di programmi specifici e avanzati algoritmi, consente di giungere a esiti articolati in tempi nettamente ridotti, definendo una sostituzione, seppur talvolta solo parziale, dell'attività e del controllo dell'uomo negli ambiti più diversificati, individuali o sociali. Questa caratteristica tecnica, tipica dell'informatica, assume rilevanza giuridico-penale e risulta funzionale al corretto inquadramento del fenomeno, interessando il giurista e, più in particolare per quel che qui rileva, il penalista[7]. Peraltro, il valore attribuito al suddetto procedimento meccanico risulta dalle stesse definizioni giuridiche presenti nelle principali fonti nazionali e sovranazionali[8].

1.1.1 La formazione di una nuova dimensione: il *cyberspace*

In ragione della profonda rivoluzione tecnologica illustrata, si sviluppa, proprio per mezzo delle nuove *ICT*, e specialmente grazie alla diffusione

sanzioni, compresa quella più drastica dell'esclusione da servizi, reti e connessioni, così da regolare, prepotentemente, i comportamenti degli utenti, dei concorrenti, dei terzi».

[7] In tal senso PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, cit., 43 s.: «Con l'"informatizzazione" l'uomo è sostituito in ambiti ed aspetti sempre più estesi ed articolati del suo agire, individuale e sociale, comprese in particolare le sue funzioni di acquisizione e memorizzazione di nuove informazioni, nonché controllo e svolgimento di attività sempre più articolate ed interdipendenti: dalla gestione di modelli previsionali in ogni settore, all'organizzazione della produzione e del lavoro, dalla selezione e gestione della pubblicità da indirizzare ad estese categorie od a singoli utenti (c.d. personalizzazione) a livello globale, fino alle ricerche statistiche, epidemiologiche, d'opinione o perfino alle diagnosi mediche, alla microchirurgia, od alla guida automatizzata di veicoli di ogni natura, comprese oggi le automobili, ecc.».

[8] A titolo esemplificativo vengono riportare le definizioni d'interesse relative all'art. 2 della Direttiva 2013/40/UE del Parlamento Europeo e del Consiglio: «Sistema di informazione: un'apparecchiatura o gruppo di apparecchiature interconnesse o collegate, uno o più dei quali svolge un trattamento automatico di dati informatici secondo un programma, nonché i dati informatici immagazzinati da tale apparecchiatura o gruppo di apparecchiature, trattati, estratti o trasmessi dagli stessi ai fini della loro gestione, uso, protezione e manutenzione; dati informatici: una rappresentazione di fatti, informazioni o concetti in una forma che può essere trattata in un sistema di informazione, compreso un programma atto a far svolgere una funzione a un sistema di informazione».

dell'automazione, una nuova e più estesa dimensione sociale ed umana che ben si esprime con il termine cyberspazio[9].

Benché non vi sia una definizione comunemente accolta[10], lo spazio cibernetico viene inteso, oggi, quale insieme di infrastrutture informatiche interconnesse, comprensivo di *hardware*, *software*, dati ed utenti, oltreché delle relative relazioni esistenti tra questi[11], come puntualizzato dall'art. 2, lett. (h) del Decreto del Presidente del Consiglio dei Ministri n. 66 del 2013[12].

Tale articolata realtà, globalmente manifestatasi, va oltre il mero concetto di Rete o *web* che, riferendosi di per sé alla mera dimensione tecnica e materiale – la quale rappresenta indubbiamente il necessario supporto che è alla base dei fenomeni menzionati –, ad oggi risulta riduttivo. In altri termini, il cyberspazio non coincide con Internet ma lo ricomprende, altresì includendo le reti di comunicazione, i sistemi informatici di elaborazione dei dati e i dispositivi mobili dotati di connessione di rete.

Il concetto di cyberspazio collega la "cibernetica"[13] alla complessa nozione di "spazio" – comunemente definito "virtuale", seppur talvolta impropriamente –,

---

[9] In argomento BALLONI, BISI, SETTE, *Principi di criminologia applicata. Criminalità, controllo, sicurezza*, Padova, 2015, 251 s. Fu William Gibson, scrittore canadese, a coniare il termine *cyberspace* nel 1982 in occasione di un suo racconto di fantascienza dal titolo *Burning Chrome* e ad inserirlo successivamente nel romanzo *Neuromancer* che lo rese noto alla collettività. L'autore identificò il cyberspazio come un luogo immaginario fatto di allucinazioni tecnologiche antitetico alla realtà; solo in seguito, a partire dalla prima metà degli anni Novanta, con l'avvento di Internet, l'espressione si è diffusa assumendo un significato ben diverso e divenendo impropriamente sinonimo di internet, ossia della Rete delle reti, benché dovesse riferirsi, più correttamente, a tutti i sistemi digitali di connessione, acquisizione e condivisione delle informazioni.

[10] V. MARTINO, *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in *Politica&Società*, 2018, 1, 63 s: secondo F.D. Kramer esisterebbero almeno ventotto diverse definizioni del termine cyberspazio, e ciò è indice del fatto che sono stati molti gli esperti che si sono cimentati nella ricerca di una quanto più corretta definizione da attribuire allo spazio cibernetico, tra i quali Daniel T.Kuehl secondo cui il c*yberspa*ce è «un dominio globale all'interno dell'ambiente informatico il cui carattere distintivo e unico è caratterizzato da un uso dell'elettronica e dello spettro elettromagnetico per creare, memorizzare, modificare, scambiare, e sfruttare le informazioni attraverso sistemi interdipendenti e interconnessi che utilizzano le tecnologie delle informazioni e delle comunicazioni».

[11] Si veda MENSI, La sicurezza cibernetica, in MENSI, FALLETTA, *Il diritto del web*, Padova, 2018, 281.

[12] V. *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale* adottata con D.p.c.m. 24 gennaio 2013, pubblicato nella Gazzetta Ufficiale 19 marzo 2013, n. 66.

[13] In argomento PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, cit., 39: il termine cibernetica, derivato dal greco "*kybernetes*" che significa "navigatore, fu coniato nel 1948 da Norbert Wiener e utilizzato già nel secolo scorso per indicare una nuova scienza

in quanto si considera come un'oggettività dinamica e multidimensionale che meglio rappresenta la pervasiva espansione del nuovo mondo, in cui ciascun essere umano è realmente, e non solo virtualmente, introdotto[14].

Si realizza una vera e propria proiezione dell'io in una nuova dimensione in cui, attraverso la traslazione delle comuni capacità di azione, nonché di interazione e di scambio, è possibile svolgere operazioni di ogni genere, tra le quali, per quel che nello specifico interessa, esplorare le zone del *deep web* o del *dark web*, ma anche più semplicemente far ricorso alle piattaforme *e-commerce* per acquistare e vendere legittimamente qualunque bene. Il cyberspazio diviene quindi un luogo imprescindibile per instaurare quotidianamente interconnessioni in ogni parte del mondo, funzionale allo sviluppo economico, culturale e sociale in generale, grazie alla presenza di opportunità di espressione, informazione e associazione.

Il *cyberspace* si presenta come una realtà complessa, contraddistinta dal dinamismo e soggetta dunque ad un costante cambiamento al passo con il progresso scientifico e tecnologico, che genera ed ha generato molteplici e talvolta deflagranti impatti sul diritto vigente, non solo penale; è un mondo prodotto dall'attività antropica, un ambiente artificiale che ha modificato le tradizionali dinamiche sociali, e il cui elemento distintivo può essere ravvisato nell'astrattezza, poiché capace di collegare tutti i dispositivi idonei, ovunque situati, ad un'unica rete, consentendo così l'interazione tra gli utenti.

L'ambiente cibernetico, difficilmente identificabile e governabile, è un luogo indefinito e privo di confini spazio-temporali i cui connotatati essenziali sono appunto ravvisabili nella dematerializzazione, aterritorialità e atemporalità, altresì funzionali a garantire l'ubiquità, l'anonimato e la pervasività.

Le condotte che si esplicano in rete si distinguono da quelle tradizionali proprio in ragione delle suddette peculiarità, le quali consentono all'utente di essere "virtualmente" presente in più luoghi informatici anche nello stesso momento, attingendo alla connessione in ogni istante e in qualunque luogo grazie all'uso di adeguati dispositivi, nonché di compiere una o più operazioni complesse contemporaneamente. È inoltre possibile pianificare lo svolgimento di un'attività

interdisciplinare, il cui proposito è risultato essere lo studio dei meccanismi con cui uomini, animali e macchine comunicano con l'ambiente esterno e lo controllano.

[14] *Ibidem*.

in tempi diversi, ed usufruire, per la sua realizzazione, delle, già menzionate, operazioni automatizzate, evitando così la necessità di un diretto contatto fra individuo e sistema informatico. Ciò comporta inevitabili problematiche legate all'applicazione dei tradizionali principi, tra i quali quello di territorialità, che richiedono l'individuazione di un luogo in cui viene posta in essere la condotta, tanto da arrivare a parlare di anarchia del *cyberspace*[15]. Ad ogni modo, l'idea di uno spazio totalmente libero dal diritto e dal controllo, sinonimo dunque di anarchia, si è, con il tempo, assolutamente escluso[16].

Tuttavia, come anticipato, si tratterebbe di una dimensione non puramente virtuale, in ragione non solo del necessario utilizzo di oggetti materiali per l'accesso ad una connessione, ma anche del fatto che sono gli individui stessi a creare e condizionare questa realtà. Il *cyberspace* avrebbe quindi una natura ibrida, poiché alla sua formazione concorrono sia elementi fisici che digitali, rendendolo allo stesso tempo reale e virtuale; questa peculiarità rifletterebbe la difficolta e l'incapacità di giungere ad un'universale e condivisa descrizione cognitiva del termine[17].

In virtù del carattere eterogeneo della natura del cyberspazio, alcuni esperti hanno ipotizzato una stratificazione di questa realtà in quattro differenti livelli: un livello fisico, costituito da dispositivi materiali che consentono il funzionamento della rete; un livello logico, che, attraverso l'unione delle diverse componenti che offrono servizi agli utenti, crea e determina la natura della piattaforma di Internet; un livello d' informazione, in cui avviene la creazione e la distribuzione dell'informazione, e la conseguente interazione tra gli utenti; un livello personale, costituito da singoli individui che realizzano siti, contenuti o pongono in essere operazioni *online*[18].

Questa rappresentazione dell'ambiente cibernetico non è universalmente condivisa, infatti alcuni studiosi, tra cui Martin C. Libicky, individuano tre diversi

---

[15] V. FLOR, *I limiti del principio di territorialità nel cyberspace. Rilievi critici alla luce del recente orientamento delle Sezioni Unite*, in *Dir. pen. proc.*, 2015, 10, 1297.

[16] In tal senso PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, cit., 41.

[17] Così MARTINO, *La quinta dimensione della conflittualità*, cit. 64.

[18] In tal senso PANATTONI, Compliance, cybersecurity *e sicurezza dei dati personali*, Assago, 2020, 7 ss.

livelli: fisico, semantico e sintattico. Il primo è costituito da elementi fisici; il secondo, collocato su un livello superiore, è composto da informazioni e indicazioni relative allo strumento informatico, quali, ad esempio, protocolli operativi; il terzo è deputato all'elaborazione dei dati presenti nelle macchine[19].

La regolare presenza degli individui nel cyberspazio è attualmente garantita dall'esistenza di dispositivi sempre più avanzati, capaci di operare ovunque, e dalla costante copertura, tendenzialmente completa, delle reti di comunicazione di dati, oltreché dalle numerose tecniche di connessione esistenti.

In rete sono presenti svariate tipologie di servizi, dall'*e-commerce* alla *digital economy*, tutto assume una nuova forma, mantenendo però inalterato, o tutt'al più migliorando, il contenuto; si realizza la trasposizione dell'intero sistema economico e sociale nel *cyberspace*, tantoché anche gli stessi servizi essenziali per il Paese vengono forniti attraverso reti telematiche, elevando così lo *standard* di qualità nell'erogazione e nell'accesso agli stessi[20].

Si parla, a tal proposito, di "infrastrutture critiche"[21], vale a dire quelle infrastrutture fondamentali per il Paese, dal cui disfacimento o disfunzione deriverebbero ripercussioni negative per l'intera Nazione, e per cui risulta necessaria un'appropriata protezione ad opera degli stessi Stati, quali principali protagonisti e garanti della sicurezza nel cyberspazio[22]. In particolare, al singolo Stato è attribuito il dovere di proteggere le reti e le infrastrutture, richiamando i diritti democratici e pretendendo il rispetto della pianificazione strategica varata da ciascun Paese anche nel dominio cibernetico, al fine di assicurare un adeguato bilanciamento tra le libertà tipiche dell'ambiente considerato e i valori rievocati.

---

[19] Sul punto MARTINO, *La quinta dimensione della conflittualità*, cit., 64 s.

[20] Così VULPIANI, *La nuova criminalità informatica. Evoluzione del fenomeno e strategie di contrasto*, in *Riv. di criminologia, vittimologia e sicurezza*, Vol. I, n.1, 2007, 4.

[21] Cfr. SARZANA DI S. IPPOLITO, *Informatica, Internet e diritto penale*, (terza edizione, riveduta, corretta ed ampliata), Milano, 2010, 25: «La convenzione delle N.U del 23 dicembre del 2002(art. n.2), afferma che per infrastrutture critiche s'intende ogni impianto, pubblico o privato, che fornisce servizi di utilità pubblica come la conduzione di acqua, l'evacuazione delle acque reflue, l'energia, il combustibile o le comunicazioni. Secondo la Comunicazione della Commissione UE, COM (2004) 702 del 20 ottobre 2004, le infrastrutture critiche consistono in infrastrutture materiali o di tecnologia dell'informazione, reti, servizi e beni il cui danneggiamento o distruzione avrebbe gravi ripercussioni sulla salute, la sicurezza ed il benessere dei cittadini oppure sul valido funzionamento delle amministrazioni pubbliche degli stati membri».

[22] V. DIRETTIVA 2008/114/CE del Consiglio dell'Unione Europea relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione, recepita dall'Italia con d.lgs. n. 61 dell'11 aprile 2011.

L'intento primario è dunque quello di contenere le minacce che, provenienti da questa nuova dimensione, comportano vulnerabilità per la sicurezza dell'intero Paese.

1.2 La minaccia cibernetica e la nascita della criminalità informatica: le origini della *cybersecurity*

Lo sviluppo tecnologico e la conseguente formazione del dominio cibernetico mostrano, oltre agli aspetti positivi sin qui richiamati, una serie di criticità tipiche della nuova dimensione e del fenomeno digitale più in generale. Tali aspetti negativi, ravvisabili in nuove forme di aggressione poste in essere da organizzazioni criminali o da singoli individui, e destinate a pubblici o privati, costituirebbero le c.d. "minacce cibernetiche", ossia condotte controindicate commesse nel cyberspazio, attraverso ovvero in danno dello stesso[23], le quali possono assumere diverse forme e connotazioni.

Più precisamente, l'art 2 n. 8 del *Cybersecurity Act* [24] definisce la minaccia informatica come «qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sulla rete e sui sistemi informativi, sugli utenti di tali sistemi e altre persone».

Come anticipato, queste minacce sono rivolte ai diritti degli utenti, alle infrastrutture fisiche, alle attività produttive o direttamente agli Stati, poiché capaci di colpire e danneggiare entità nazionali più o meno ampie.

Le conseguenze proprie di azioni minacciose commesse nel cyberspazio sono rinvenibili nella realtà fisica, in cui però, a causa dell'anonimato, risulta complesso svolgere le consuete attività di investigazione e di identificazione del colpevole.

La manifestazione delle suddette azioni è infatti caratterizzata dalla variabilità, in ragione della continua evoluzione, e dall'asimmetricità, poiché sussiste il potenziale rischio per ciascun sistema informativo di essere colpito da qualunque luogo e a qualsivoglia distanza, purché vi sia un accesso alla rete; tali atti sono soliti sfruttare anche l'unica e minima vulnerabilità tecnico-organizzativa

[23] Cfr. PRESIDENZA DEL CONSIGLIO DEI MINISTRI, Cyberbook. *Il glossario della sicurezza*, in *www.sicurezzanazionale.gov.it.*

[24] In tal senso PANATTONI, Compliance, cybersecurity *e sicurezza,* cit., 25.

dei più sofisticati e protetti sistemi, non permettendo un'adeguata risposta difensiva in virtù della velocità d'azione.

Il moltiplicarsi delle minacce, dovuto principalmente all'esponenziale crescita delle aree di debolezza tipiche del mutevole contesto tecnologico, rende sempre più difficoltosa l'esistenza di sistemi informativi totalmente sicuri e protetti, e ciò anche in ragione della continua trasformazione di tali forme di aggressione. È l'essenza stessa del dominio cibernetico a rendere le minacce, che in esso si verificano, estremamente insidiose.

In base agli attori e alle finalità perseguite possono essere individuate molteplici tipologie di minacce, le quali assumeranno dunque una diversa natura. A tal proposito si è soliti distinguere quattro macro-categorie[25]:

la criminalità cibernetica, che consta della totalità delle attività con finalità criminali, la cui più incisiva, seppur generale, definizione è stata fornita dalla Commissione Europea nel 2007, e così testualmente riportata «atti criminali commessi contro reti di comunicazioni elettroniche e sistemi di informazione o avvalendosi di tali reti e sistemi»[26];

lo spionaggio cibernetico, che riguarda l'indebito ottenimento di dati o informazioni sensibili;

il terrorismo cibernetico, che risulta dal complesso di comportamenti ideologicamente motivati, volti ad influenzare e colpire uno Stato o un'organizzazione internazionale;

la guerra cibernetica, quale insieme di operazioni militari organizzate e poste in essere nel cyberspazio per conseguire effetti nel detto ambiente. Segnaliamo che, benché il concetto di *cyber-warfare* sia stato affrontato in molti documenti dell'UE, esso si considera argomento di esclusiva competenza della NATO e dei suoi Stati Membri.

Emerge chiaramente, da questa breve disamina, che la criminalità informatica, o più in generale cibernetica, poiché si origina e manifesta globalmente

[25] PRESIDENZA DEL CONSIGLIO DEI MINISTRI, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, Dicembre 2013, *www. sicurezza nazionale.gov.it*, 12 s.

[26] Commissione europea, *Verso una politica generale di lotta contro la cyber-criminalità*, COM(2007)267, Bruxelles.

nella Rete, è una delle conseguenze, nonché finalità, proprie degli attacchi di cui si sostanziano le suddette minacce.

La rivoluzione cibernetica ha dunque consentito l'origine di nuovi comportamenti illeciti che pregiudicano e violano seriamente i diritti e gli interessi dei singoli e della collettività. Queste nuove forme di prevaricazione, intimidazione e controllo delle informazioni, della volontà e dell'individuale o collettiva capacità di scelta hanno determinato la nascita di nuovi conflitti, agevolando la diffusione di condotte penalmente inammissibili, ed è proprio in questa fase della trattazione, dedicata alle minacce cibernetiche e alla nascita della criminalità informatica, che è più opportuno parlare di "diritto penale dell'informatica".

Nel campo più propriamente penale, infatti, alle nuove forme di criminalità informatica, o cibernetica, si associano innovative, seppur talvolta complesse e insufficienti, tecniche investigative e di raccolta delle prove, grazie all'utilizzo di strumenti moderni e all'avanguardia.

Nei primi anni Sessanta il fenomeno della delinquenza informatica è stato oggetto di studio soprattutto della criminologia, mentre l'intervento dei giuristi è avvenuto successivamente, poiché inquadrare l'illecito informatico dal punto di vista giuridico risulta più complicato che dal punto di vista descrittivo-criminologico.

Con il tempo, questo tipo di criminalità si è evoluto in modo considerevole fino a che, con l'avvento di Internet[27], ha raggiunto l'apice della pericolosità; si presenta come un fenomeno maggiormente raffinato rispetto alle classiche figure di reato[28].

Le eclatanti o, talora, tacite nuove forme di aggressione e le originali insidie della criminalità informatica e cibernetica che si collocano nel *cyberspace* sono attribuibili non solo ai *cyber*-criminali, ma anche alle moderne concentrazioni di

[27] Cfr. BALLONI, BISI, SETTE, *Principi di criminologia applicata*, cit., 252 s.: «Internet, concepito negli anni Sessanta del secolo scorso come progetto di difesa in ambito statunitense, si è infatti progressivamente allontanato dalle finalità militari per le quali era stato congeniato imponendosi come mezzo di comunicazione di massa diffuso su scala planetaria».

[28] V. SARZANA DI SANT'IPPOLITO, *Problemi vecchi e nuovi nella lotta alla criminalità informatica*, in PICOTTI (a cura di), *Il diritto penale dell'informatica nell'epoca di internet*, Padova, 2004, 3 s.

poteri createsi nel *web*, che costantemente minacciano diritti e interessi meritevoli di un'idonea tutela penale.

Dinanzi a tale esigenza si impone la necessità di costituire sistemi equilibrati e armoniosi d'incriminazioni e sanzioni penali, fortificando la cooperazione a livello internazionale e includendo singoli Stati, industrie, enti e associazioni.

Occorre innanzitutto definire i comportamenti considerati penalmente rilevanti nel dominio cibernetico, rispetto ai quali quindi si giustifica la previsione delle suddette sanzioni penali, per rendere effettivo il principio basilare secondo cui "ciò che è illecito *offline* non è considerato lecito *online*", nonostante le differenti forme o le particolari modalità di esternazione.

Dunque, dal punto di vista penale, un approccio conservatore risulta inappropriato, poiché l'utilizzo degli strumenti tradizionali di estensione ermeneutica delle norme vigenti e l'impiego delle classiche categorie dogmatiche, come accennato in precedenza, non risultano adeguati ai nuovi fenomeni, obbligando la disciplina penale a riorganizzarsi e rinnovarsi per adattarsi ai complessi rapporti che si sviluppano nel cyberspazio. Sorge quindi la necessità di definire un quadro giuridico generale che contenga criteri e regole d'imputazione della responsabilità penale conformi alla nuova dimensione, al fine di superare le insicurezze applicative e i contrasti interpretativi dovuti alla digitalizzazione.

In altre parole, il penalista deve tenere conto delle particolarità della realtà cibernetica e delle peculiarità che acquisiscono le azioni dei singoli e dei gruppi nel momento in cui si dematerializzano nel *cyberspace*; gli attori del nuovo mondo sono gli utenti, i quali non solo diventano autori di comportamenti discutibili, diffondendo contenuti in rete, ma sono anche i destinatari di tali informazioni interattive; assume rilevanza inoltre, in questo contesto, la complessa categoria degli *Internet Service Providers*, il cui denominatore comune risulta difficilmente individuabile.

Come preannunciato, nell'ottica processuale diviene necessario elaborare specifiche regole relative alle misure cautelari adottabili o alle tecniche di ricerca, raccolta ed utilizzabilità delle prove c.d. "elettroniche", tutelando altresì, in tali situazioni d'ingerenza da parte delle autorità inquirenti, i diritti e le libertà fondamentali.

La crescente interazione tra gli utenti, nei primi anni del nuovo millennio, ha indotto gli individui a condividere informazioni in *forum, social networks e blogs*, definendo il c.d. "*Web* 2.0"; la multimedialità delle comunicazioni, nonché il progresso grafico e le maggiori opportunità di connessione hanno determinato il successivo passaggio al "*Web* 3.0", mentre lo sviluppo di sempre più sofisticati algoritmi di elaborazione ha prefigurato l'attuale "*Web* 4.0", governato dall'intelligenza artificiale, in cui gli utenti creano e propagano contenuti di ogni tipo, da cui vengono tratti dati più o meno sensibili che li riguardano. Il mondo reale si intreccia indissolubilmente con quello cibernetico, in cui si creano gli *alter ego* digitali che rimpiazzano in parte gli individui.

Da quanto appena detto emerge un'ampia libertà d'azione, la quale però riflette una altrettanto estesa possibilità di commissione di comportamenti criminosi. In altre parole, quindi, a ciascun utente è riconosciuta una maggiore capacità d' espressione, sviluppo e comunicazione, grazie al facilitato accesso al cyberspazio, ma, contestualmente, anche una più alta possibilità di divenire autore o vittima di offese ed illeciti.

Gli interessi e i diritti da tutelare sono innumerevoli, dalla reputazione alla riservatezza, dalla sicurezza informatica all'esclusiva sui prodotti dell'ingegno, non tralasciando la salvaguardia delle libertà fondamentali, tra le quali il divieto di discriminazioni o il più generale interesse al corretto svolgimento degli scambi.

I crimini perpetrati nello spazio producono, inoltre, un profondo danno economico, poiché in rete sono diffuse e conservate innumerevoli quantità di dati aziendali o riguardanti la condizione patrimoniale degli individui, oltreché informazioni economiche delicate relative ad attività finanziaria e commerciale; tale condizione rende gli attacchi cibernetici potenzialmente lucrativi. Risultano dunque esposti a grave rischio non solo i singoli, ma anche le imprese, gli istituti finanziari, bancari e gli enti economici nazionali e internazionali, essendo gli stessi fonti di dati digitali personali, industriali e finanziari; ciò che viene compromessa è dunque la *business continuity*[29].

[29] In argomento MENSI, *La sicurezza cibernetica*, cit., 284.

I soggetti più deboli, quali potenziali autori o vittime della criminalità informatica, sono proprio i minori, poiché maggiormente esposti ai gravi fenomeni del *cyber*-bullismo o della pedopornografia.

Senza voler anticipare quanto si dirà poi, sembra opportuno precisare la vasta portata del fenomeno che, interessando il legislatore nazionale, ha portato all'introduzione della prima legge contro la criminalità informatica nel 1993; con il tempo, però, la delinquenza nel *cyberspace* ha assunto dimensioni transnazionali, per cui è riduttivo parlare di repressione solo a livello nazionale.

Dalle tradizionali forme di manifestazione della criminalità, volte a colpire valori intrinsecamente ricollegabili alla persona, come l'integrità fisica, si è arrivati a considerare fenomeni criminali in cui la tecnologia informatica e comunicativa, nonché l'insieme di beni immateriali da essa originati acquisiscono un ruolo primario nell'ordinamento giuridico, sia come bersaglio dell'attività criminosa, sia come strumento di consumazione del reato.

È opportuno, inoltre, tenere presente i milioni di utenti che navigano nel *World Wide Web* per capire quanto enorme ed esteso possa essere l'impatto criminale sul c.d. "villaggio globale"[30].

Tuttavia, considerate le specifiche caratteristiche della realtà digitale, i soli meccanismi tradizionali di contrasto si dimostrano inefficaci, ritenendosi indispensabile ricorrere all'impiego di strumenti preventivi nella lotta al crimine informatico, per combattere alla fonte le minacce cibernetiche, laddove possibile. Dunque, al fine di contrastare incisivamente simili minacce, è necessario adottare un quadro di misure di sicurezza delle reti e dei sistemi informatici basate sulla prevenzione e sulla collaborazione tra le diverse autorità interessate; infatti i soggetti che operano nel cyberspazio, ovverosia gli Stati in cooperazione con i privati, hanno innanzitutto l'onere di impegnarsi per adeguare costantemente *standard* e protocolli di sicurezza al mutevole contesto operativo, e di garantire pertanto la difesa dei sistemi, poiché, alle volte, la causa degli attacchi è data proprio dall'inefficace protezione o dal mancato adempimento dei requisiti necessari.

[30] In argomento VULPIANI, *La nuova criminalità informatica*, cit., 4.

Riconoscere preventivamente le suddette vulnerabilità e sopperire alle eventuali mancanze nell'ambito della sicurezza dei sistemi consente una successiva diminuzione dei costi per la messa a punto dei relativi controlli.

Come si avrà modo di specificare, garantire la sicurezza fisica, logica e procedurale nel dominio cibernetico implica la predisposizione di un idoneo sistema di prevenzione, basato sull'analisi del rischio e della gestione dello stresso; a tal proposito si è soliti parlare di *cybersecurity*, quale articolato concetto di cui non esiste un'univoca definizione, da intendersi come capacità di difendere il *cyberspace* dalle minacce cibernetiche , proteggendo in particolare gli *asset* fisici e la totalità delle relative informazioni.

Da quanto fin qui riportato, è facilmente intuibile il rilievo che assume la *cybersecurity* nel contesto globale, poiché «rappresenta la risposta politica, economica, e normativa agli attacchi realizzati nello spazio virtuale, anche in termini di valutazione e gestione del rischio informatico»[31].

Con riguardo alle definizioni internazionali, *l'International Telecommunication Union* delle Nazioni Unite definisce la *cybersecurity* quale «insieme di strumenti, interventi, concetti, linee guida, impostazioni della gestione del rischio, azioni, pratiche, procedure e tecnologie che possono essere utilizzate per proteggere lo spazio e la struttura cibernetica e i loro utilizzatori»[32].

Secondo quanto stabilito dall' Unione europea nel 2013, invece, la *cybersecurity* allude a «le misure di salvaguardia e le azioni che possono essere utilizzate per proteggere il dominio cibernetico, da quelle minacce che sono associate o che possono danneggiare le sue reti interdipendenti e la sua infrastruttura informativa. La sicurezza informatica si impegna a preservare la disponibilità e l'integrità delle reti e delle infrastrutture e la riservatezza delle informazioni in esse contenute»[33].

Ancora, in base a ciò che è previsto nelle fonti italiane, e più precisamente stando a quanto emerge dal *Framework* nazionale per la *cybersecurity* del 2015, la definizione di tale concetto è solita riferirsi a «quella pratica che consente a

---

[31] V. SEVERINO, *Standard globali in difesa della trasformazione digitale*, in *www.ilsole24ore.com*, 29 marzo 2019.

[32] Cfr. MENSI, *La sicurezza cibernetica*, cit., 285.

[33] Così PANATTONI, Compliance, cybersecurity *e sicurezza*, cit., 5.

un'entità (ad esempio, organizzazione, cittadino, nazionale ecc.) la protezione dei propri *asset* fisici e la confidenzialità, integrità e disponibilità delle proprie informazioni dalle minacce che arrivano dal *cyberspace*»[34]. In altri termini, quindi, in un siffatto panorama si rende necessaria la definizione di una cornice normativa adeguata, tesa alla prevenzione e funzionale a respingere le minacce nel *cyberspace*, che coinvolga soggetti pubblici e privati.

La *cybersecurity*, perciò, raffigura il contesto in cui si predispongono le regole che disciplinano le relazioni tra i diversi soggetti che agiscono nel cyberspazio, e il cui intento principale è da ravvisarsi nella tutela di pubblici o privati da possibili eventi dannosi perpetrati attraverso il funzionamento o l'impiego di mezzi informatici; essa costituisce un indispensabile strumento globale di protezione e di garanzia dei diritti e delle libertà fondamentali che in rete rischiano di essere offesi, infatti ad essa viene assegnato il delicato compito di esaminare le informazioni e i dati che la tecnologia consente di raccogliere, elaborare, immagazzinare e trasmettere.

La sicurezza cibernetica assume un inevitabile carattere sovranazionale e dematerializzato, ed è destinataria di molteplici investimenti in termini di risorse economiche, tecniche e conoscitive.

I concetti chiave della sicurezza informatica, e più in generale cibernetica, sono la confidenzialità, l'integrità e la disponibilità, le quali costituiscono la c.d. "triade *C.I.A*" (*confidentiality, integrity, availiability*). Il suddetto acronimo si riferisce non solo ai dati e alle informazioni, ma anche ai sistemi e alla rete, affinché queste possano essere considerate sicure[35].

La confidenzialità è relativa alla non disponibilità o divulgabilità delle informazioni, e dipende dalla capacità di proteggere i dati da entità non abilitate all'accesso; l'integrità riguarda l'accuratezza e la completezza, nonché l'abilità di impedire la modifica non autorizzata delle informazioni; la disponibilità si riferisce

[34] *Ibidem*.

[35] Per approfondire v. FLOR, Cybersecurity *ed il contrasto ai* cyber-attacks *a livello europeo: dalla CIA*-Triad protection *ai più recenti sviluppi*, in *Riv. dir. Internet*, 2019, 3, 453 ss.

alla garanzia di accesso e utilizzabilità dei dati e delle informazioni in qualunque momento e su richiesta di entità legittimate[36].

Ad ogni modo, in un ambito esteso come quello della *cybersecurity*, queste caratteristiche non sembrano sufficienti, ed è pertanto necessario fare riferimento anche alle ulteriori proprietà tipiche della sicurezza dei dati, delle informazioni e delle tecnologie dell'informazione e della comunicazione, le quali sono: l'autenticità, secondo cui una cosa è ciò che dichiara di essere; la responsabilità; il non-disconoscimento, da individuarsi nell'abilità di dimostrare l'occorrenza dell'evento o dell'azione che si è detto tale, oltreché l'entità da cui ha avuto origine; l'affidabilità, carattere per cui il comportamento tenuto e il risultato avuto sono coerenti e conformi a quelli voluti[37].

La discussione relativa al concetto della cybersicurezza si origina negli Stati Uniti d'America, dove, intorno agli anni Settanta, nascono le prime questioni circa lo sviluppo tecnologico e la gestione delle relative innovazioni. Solo negli anni successivi l'attenzione si è spostata più propriamente sulla tutela delle informazioni trasmesse per mezzo del computer e delle tecnologie informatiche. Ma è grazie all'evoluzione delle suddette tecnologie, nonché all'avvento della rete Internet, che il *focus* si sposta sulle vulnerabilità che contraddistinguono non solo i dispositivi informatici di per sé, ma anche le reti e i *networks*; in ragione di ciò, la questione relativa alla *cybersecurty* perde il carattere meramente tecnico-informatico e assume una connotazione sociopolitica.

Ad oggi il dibattito sul tema riguarda principalmente le già citate infrastrutture critiche e le organizzazioni, in ragione della sempre maggiore dipendenza della società dalla tecnologia.

È opportuno, inoltre, sottolineare l'ampiezza che connota il termine *cybersecurity* rispetto alla mera *Information Security* e all'*ICT security*, proprio in virtù del fatto che la sicurezza cibernetica si riferisce oltre che a queste ultime anche alla Rete, e dunque ad una più estesa dimensione sociale e politica, cogliendo aspetti e problematiche persino a carattere politico-sociale; per tali ragioni, dunque, quello

[36] *www.sicurezzait.gov.it.*

[37] In argomento PANATTONI, Compliance, cybersecurity *e sicurezza*, cit., 6.

della *cybersecurity* è un concetto più articolato con cui si è soliti riferirsi a un *quid pluris* rispetto alla mera sicurezza informatica o all' *ICT security*.

Quanto sin qui esposto è così sintetizzabile: «la *cybersecurity* consiste nel rendere il *cyberspace* (spazio costituito da informazioni, *ICT, network* e infrastrutture *ICT*) sicuro»[38].

Negli anni sono state adottate molteplici iniziative a livello nazionale e sovranazionale per innalzare il livello di sicurezza, gestire il rischio e limitare la debolezza dei sistemi informatici, contribuendo alla creazione dell'attuale quadro giuridico e normativo di riferimento, di cui si dirà meglio in seguito.

Si tratta di un tema che, negli ultimi tempi, ha assunto un valore strategico anche per l'Unione Europea; la Commissione, infatti, nel 2001, si è adoperata per l'adozione di una comunicazione sulla criminalità informativa[39], relativa alla protezione delle infrastrutture e alla repressione dei reati informatici, in seguito integrata da un'ulteriore Comunicazione[40], sempre nello stesso anno, concernente la *network information security*, ossia «la capacità di una rete o di un sistema d'informazione di resistere, ad un determinato livello di riservatezza, ad eventi imprevisti o atti dolosi che compromettono la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati o trasmessi e dei servizi forniti o accessibili tramite la suddetta rete o sistema»[41]. Tale provvedimento si mostra funzionale a tipizzare le differenti minacce pregiudizievoli alla sicurezza delle reti[42].

---

[38] *Ivi*, 8.

[39] In argomento MENSI, *La sicurezza cibernetica*, cit., 287 che richiama COM(2000) 890 del 26 gennaio 2001, Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informativa.

[40] In argomento MENSI, *La sicurezza cibernetica*, cit., 287 che richiama COM (2001) 298 del 6 giugno 2001, Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo.

[41] Sul punto MENSI, *La sicurezza cibernetica*, cit., 286 che richiama COM (2001) 298 del 6 Giugno 2001, 9

[42] v. MENSI, *La sicurezza ciberne*tica, cit., 286.

L'attenzione europea per il fenomeno si è ulteriormente manifestata con l'emanazione di molteplici Direttive[43] e Comunicazioni[44], alcune delle quali[45], ancora una volta, finalizzate ad assicurare la protezione delle infrastrutture critiche informatizzate.

La Commissione Europea, nel 2013, ha inoltre evidenziato che gli incidenti concernenti la sicurezza informatica aumentano costantemente di frequenza ed entità, diventando sempre più articolati e complessi da contrastare.

Ogni anno, a livello globale, l'elevata percentuale di sinistri causati dalla criminalità informatica provoca rilevanti perdite economiche, rispetto alle quali vengono condotte regolarmente indagini e predisposte accurate statistiche.

Per quel che riguarda la distribuzione delle competenze si riconosce all'Unione Europea un ruolo secondario, di integrazione e armonizzazione delle iniziative nazionali, essendo affidata agli Stati membri la titolarità delle maggiori responsabilità in tema di *cybersecurity*. Infatti, solo di recente, dinanzi alla necessità di definire un'adeguata cornice giuridica per garantire la protezione delle reti e delle informazioni attraverso la tutela delle infrastrutture critiche informatizzate, e per contrastare la *cyber*-criminialità, nonché per regolamentare le comunicazioni elettroniche, sono state predisposte numerose iniziative da parte dell'Unione europea. Quest'ultima ha inoltre definito due precisi obiettivi da realizzare: aumentare la consapevolezza dei rischi legati alla *cybersecurity*; affinare le reazioni nazionali ed europee agli eventuali attacchi o incidenti informatici[46].

Nel perseguire il primo obiettivo la Commissione Europea incentiva il dialogo tra gli Stati membri e le Istituzioni Europee, ma anche tra i vari *stakeholder*, pubblici o privati, del campo.

---

[43] V. MENSI, *La sicurezza cibernetica*, cit., 287. In quest'ambito assume rilevanza il "pacchetto" delle direttive del 2002 concernente le comunicazioni elettroniche, successivamente modificate dalla direttiva 2009/136/CE e dalla direttiva 2009/140/CE, che richiede a ciascuno stato membro di adottare misure idonee ad assicurare la sicurezza delle reti.

[44] V. MENSI, *La sicurezza cibernetica*, cit., 287 che richiama: COM(2000) 130 dell'8 marzo 2000, eEurope: Una società dell'informazione per tutti; COM(2002) 263 del 28 maggio 2002, eEurope 2005: una società dell'informazione per tutti.

[45] V. MENSI, *La sicurezza cibernetica,* cit., 287 che richiama: Commissione europea, Una strategia per una società dell'informazione Sicura – "Dialogo, partenariato e responsabilizzazione", COM(2006) 656, Bruxelles, 3; Direttiva 2008/114/CE del Consiglio dell'8 dicembre 2008 relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione.

[46] *Ivi*, 288.

A tal proposito assume rilevanza l'istituzione, nel 2004, dell'Agenzia Europea per la sicurezza delle reti e dell'informazione, anche detta *ENISA*[47], quale organismo *ad hoc* che costituisce sostanzialmente una piattaforma per il confronto e lo scambio di informazioni tra tutti gli attori del settore coinvolti. All'ENISA, inoltre, è affidato il delicato ruolo di fornire consigli tecnici alle autorità nazionali ed europee, nonché quello di formare ed estendere una cultura a proposito della sicurezza delle reti, contribuendo a sostenere un corretto andamento del mercato interno[48].

Il Regolamento 2019/881/UE[49], meglio noto come *Cybersecurity Act*, ridefinisce l'organizzazione e potenzia il funzionamento dell'ENISA, al fine di creare uno schema europeo di certificazione della sicurezza informatica delle tecnologie dell'informazione e della comunicazione, volto a semplificare il commercio digitale all'interno dell'Unione, stabilendo *standard* di sicurezza comuni per garantire l'affidabilità dei prodotti[50].

La strategia europea, volta ad accrescere la protezione dei beni giuridici minacciati dal *cybercrime*, si fonda sulla cooperazione tra il settore pubblico e privato, e sul concetto di *cyber-resilience*, il quale è antitetico alla teoria di militarizzazione su cui si basa, al contrario, la *cybersecurity* statunitense.

La *cyber-resilience* nasce dall'esigenza di realizzare un *security framework* teso alla prevenzione dei rischi, e si sostanzia dei seguenti criteri[51]: instaurare una stabile collaborazione tra Istituzioni Europee e Stati membri, individuando obiettivi e politiche comuni; definire congiuntamente norme, e più in generale regole, di

[47] È l'acronimo di *European Network and Information Security Agency*.

[48] Cfr. Regolamento (UE) n. 526/2013 del Parlamento europeo e del Consiglio, del 21 maggio.

[49] Il Regolamento 2019/881/UE, concernente la certificazione della sicurezza cibernetica per le ICT, abroga Il Regolamento (UE) n. 526/2013 del Parlamento europeo e del Consiglio, del 21 maggio 2013.

[50] Cfr. PANATTONI, Compliance, cybersecurity *e sicurezza*, cit.,13 s.: «Il quadro prevede, ai sensi dell'art. 46, par. 2, "un meccanismo volto a istituire sistemi europei di certificazione della cibersicurezza e ad attestare che i prodotti, servizi TIC e processi TIC siano conformi a determinati requisiti di sicurezza al fine di proteggere la disponibilità, autenticità, integrità o riservatezza dei dati conservati, trasmessi o trattati o le funzioni o i servizi offerti da tali prodotti, servizi e processi o accessibili tramite essi per tutto il loro ciclo di vita"».

[51] Sul punto CHRISTOU, *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy, Palgrave Macmillan*, 2016, citato in MENSI, La sicurezza cibernetica, cit., 290.

sicurezza; favorire la crescita e la promozione della cultura della *cybersecurity* ad ogni livello.

Altra importante misura europea adottata in materia di sicurezza informatica e cibernetica è la Direttiva 2013/40/UE[52], avente ad oggetto gli attacchi contro i sistemi di informazione, e il cui intento principale consiste nell'armonizzare il diritto penale degli stati membri; la Direttiva constata che le più importanti lacune e differenze presenti nel diritto e nelle procedure penali degli Stati membri impediscono un'efficace e produttiva collaborazione in materia.

È stato inoltre istituito, presso l'*Europol*, il Centro europeo per la lotta alla criminalità informatica[53]; si tratta di un centro di supporto operativo, investigativo e forense che attinge alle risorse degli Stati membri per contrastare le minacce poste in essere dai *cyber* criminali.

Pur non volendo anticipare il quadro normativo di riferimento, che sarà oggetto di un successivo approfondimento, è degna di nota la Direttiva 1148/2016/UE, c.d. Direttiva NIS, quale fondamento imprescindibile nel settore della sicurezza cibernetica.

Da quanto sin qui richiamato emerge che la *cybersecurity*, non essendo una mera questione tecnico-informatica, non può essere assicurata solo attraverso la tecnologia, infatti non esistono *hardware* o *software* in grado di garantire una completa sicurezza informatica. Specialmente a causa della costante evoluzione che caratterizza le modalità di aggressione impiegate dai *cyber*-criminali, nessun sistema informativo o comunicativo può considerarsi invulnerabile. Per completezza espositiva, è necessario precisare che tale debolezza è propria di tutti i sistemi, non solo di quelli appartenenti ai singoli individui, ma anche di quelli di uso o proprietà delle imprese; in tale ambito si è soliti ricorrere allo strumento della *compliance*, poiché quello della cybersicurezza è un problema che si risolve in un

[52] V. Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, con termine di recepimento fissato al 4 settembre 2015, sostituisce la decisione quadro 2005/222/GAI del Consiglio, in G.U.U.E. 14 agosto 2013, n. L. 218. Si veda ENISA, The Directive on attacks against information systems. A Good Practice Collection for the implementation and application of this Directive, www.coe.int, come indica MENSI, *La sicurezza cibernetica*, cit., 290.

[53] V. MENSI, *La sicurezza cibernetica*, cit., 292: il Centro europeo per la lotta alla criminalità informatica (EC3) è stato inaugurato l'11 gennaio 2013. Commissione europea – IP/13/13, 9 gennaio 2013.

processo interno all'azienda, fatto di profili organizzativi, tecnologici, giuridici ed economici. Una corretta gestione interna del *cyber-risk* sta diventando determinante soprattutto a causa della sempre maggiore dipendenza delle aziende dalle tecnologie informatiche e telematiche, infatti ad oggi, nell'era della digitalizzazione delle realtà imprenditoriali, investire in *cybersecurity* è diventato per esse una priorità. Dunque, l'accresciuta debolezza dei sistemi e delle reti, nonché i pericoli derivati, quali effetti collaterali dello sviluppo tecnologico, e, in particolare, della comparsa di Internet e della diffusione delle moderne apparecchiature, possono essere per la maggior parte evitati, o comunque prevenuti, attraverso la scelta di appropriate politiche di sicurezza sia nel settore pubblico che in quello privato.

Come si evince, la *cybersecurity*, al fine di limitare le vulnerabilità del settore, sia a livello europeo che a livello nazionale, esige la predisposizione di un piano di prevenzione *ad hoc*, che si compone di tre fasi: la prima, relativa all'analisi, alla gestione e all' attenuazione del rischio; la seconda, concernente l'adozione di una serie di misure di sicurezza fisica, logica e procedurale [54]; la terza, riguardante la formazione, la sensibilizzazione e la consapevolizzazione degli utenti, quali aspetti imprescindibili[55].

La mancanza o la parziale attuazione delle regole di sicurezza[56] possono produrre gravi conseguenze per i singoli e per la collettività, per cui servirsi di misure unicamente repressive per scoraggiare i *cyber*-criminali, ricorrendo agli

[54] In argomento PRESIDENZA DEL CONSIGLIO DEI MINISTRI, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, cit., 17: le misure di tipo fisico si riferiscono alla verifica degli accessi, al fine di consentirli solo ai soggetti legittimati, e alla tracciabilità delle operazioni svolte nell'ambiente di lavoro, cosi da poter difendere gli apparati da qualunque forma di danneggiamento o furto; le misure di tipo logico riguardano l'utilizzo di prodotti certificati, per rimediare all' uso di prodotti e servizi tecnologici di fornitori esteri, considerati più a rischio, l'impiego di sistemi di cifratura, firma digitale, autenticazione e identificazione degli utenti, il tracciamento degli accessi e delle attività realizzate in rete dagli utenti, nonché l'adozione di moderni software antivirus; le misure di tipo procedurale attengono a norme e procedure tese a regolare il processo di sicurezza, stabilire i ruoli, i compiti e le responsabilità di gestione, oltreché a controllare l'attendibilità degli apparati usati e ad adottare speciali procedure per implementare la c.d. "*cyber defence"*.

[55] *Ivi*, 16 s.

[56] V. SARZANA DI S. IPPOLITO, *Informatica, Internet e diritto penale,* cit., 288 s.: le misure di sicurezza hanno essenzialmente l'obbligo di adempiere a specifiche funzioni, le quali, secondo il Prof. Sieber, sarebbero le seguenti: «dissuadere in generale le persone dal compiere o dal tentare di compiere atti non autorizzati;-impedire la commissione di veri e propri delitti informatici; permettere l' individuazione e la scoperta dell' origine degli atti delittuosi; - minimizzare gli effetti ed i danni dei delitti informatici; assicurare il rispetto delle regole legali, in particolare in materia di protezione della vita privata, e proteggere gli interessi pubblici e sociali».

strumenti penalistici, sembra insufficiente, anche in ragione della nota difficoltà di individuazione e perseguimento dei crimini informatici; alla luce di quanto esposto, sembrerebbe essere la prevenzione il miglior modo per assicurare la sicurezza e tutelare gli utenti e le infrastrutture, ferma restando l'esigenza di un idoneo sistema penale di repressione[57] .

L'intero sistema di *cybersecurity, dunque,* ruota intorno a tre fattori: la rilevanza delle fonti autoregolamentari; l'individuazione delle fonti di rischio; l'adozione di misure tecniche e organizzative adeguate a contenere ed ostacolare il rischio individuato.

Quindi, per concludere, le minacce cibernetiche e la criminalità informatica si contrastano efficacemente innanzitutto con la prevenzione e solo successivamente con la repressione[58] .

1.2.1 I *cyberattacks* e le tipologie di attacco

Gli attacchi cibernetici sono definiti come «azioni più o meno automatizzate sulle reti da parte di singoli individui o organizzazioni, statuali o non, finalizzate a distruggere , danneggiare o ostacolare il regolare funzionamento dei sistemi, delle reti o dei sistemi attuatori di processo da essi controllati ovvero a compromettere l'autenticità, l'integrità , la disponibilità e la riservatezza dei dati ivi custoditi o che vi transitano»[59], e sono soliti compromettere la fiducia degli utenti nelle tecnologie dell'informazione e della comunicazione.

Queste tipologie di attacchi sfruttano tutti i tipi di vulnerabilità, organizzative, di processo o tecniche, e talvolta anche cumulativamente.

Nello specifico, le vulnerabilità organizzative e di processo sono dovute principalmente alla mancata adozione di misure protettive, quali *best practices* o aggiornati *anti-virus,* nonché all'assenza o all'errata attuazione di misure di sicurezza fisiche; le vulnerabilità tecniche sono riconducibili, invece, a difetti di

[57] *Ivi,* 287 s.

[58] *Ibidem*.

[59] In argomento PRESIDENZA DEL CONSIGLIO DEI MINISTRI, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico, cit.,* 11.

sicurezza del *software* applicativo, o dei protocolli di comunicazione. Ad ogni modo, in tutti e tre i casi le conseguenze potrebbero divenire piuttosto gravi[60] .

Gli attacchi possono rivolgersi verso *target* eterogenei, tra i quali i privati, le infrastrutture critiche e i sistemi finanziari e di pagamento. Si tratta di destinatari vulnerabili, o per meglio dire vittime, alcuni dei quali se soggetti ad attacco possono compromettere l'assetto sociale ed economico del Paese.

Benché le infrastrutture critiche costituiscano obiettivi più ambiziosi ed elevati, in quanto trattasi di settori di vitale importanza per gli interessi nazionali, inevitabilmente connessi al sostentamento della società, i bersagli più comuni sono ad oggi rappresentati dai privati e dalle piccole realtà imprenditoriali, poiché sempre più spesso disinformati e disorganizzati in materia.

A volte, tuttavia, gli attacchi potrebbero essere generalizzati, e quindi non mirati: in tale situazione, secondo quanto previsto dall'Agenzia europea per la *cybersecurity*, essi si diffonderebbero contagiosamente nel *web*, mantenendosi più a lungo o non scomparendo per nulla. La ragione che si cela dietro una simile protrazione del rischio risiede nella disorganizzazione, nel mancato impiego e nello scorretto utilizzo, da parte della gran parte degli utenti pubblici e privati, delle misure tecniche di *cyber*-sicurezza[61].

I suddetti attacchi possono essere compiuti attraverso diverse modalità d'azione, suddividendosi così in attacchi semplici, ossia realizzati per mezzo di una singola operazione, e attacchi complessi, vale a dire posti in essere tramite una serie di operazioni tra loro connesse.

I *cyberattacks*, inoltre, possono essere distinti in base all'oggetto dell'attacco, il quale può essere: il sistema informatico o le infrastrutture fisiche o logiche, trattandosi in tal caso di attacchi attivi, funzionali ad alterare o danneggiare il sistema informatico o le sue infrastrutture, inclusi i *devices* collegati; i dati e le informazioni – in questo caso gli attacchi vengono denominati passivi, poiché volti ad acquisire o utilizzare indebitamente, alterare ovvero danneggiare dati o informazioni, senza compromettere i sistemi o le infrastrutture su cui sono memorizzati.

[60] *Ivi*, 16.

[61] Sul punto v. PANATTONI, Compliance, cybersecurity e sicurezza, cit., 27.

Ulteriore differenziazione può effettuarsi in virtù delle modalità di realizzazione dell'attacco; si è a tal proposito soliti distinguere tra: attacco fisico, il quale consiste in attività maligne rivolte contro le infrastrutture fisiche, quali computer, dispositivi informatici o *hardware i*n generale; attacco sintattico che consta di attività maligne indirizzate contro le soluzioni *software*, fondamentali per l'operatività dei sistemi e delle reti; e, infine, attacco semantico, costituito da attività maligne che influiscono sulle interazioni tra l'individuo e la macchina, nella modifica delle informazioni esatte e nella divulgazione di informazioni errate[62].

Alcuni attacchi sono eseguibili con violenza, danneggiando i sistemi informatici, le informazioni, i dati o i *software*, altri invece sono attuabili per mezzo di una condotta fraudolenta, richiedendo in tal caso la cooperazione artificiosa della vittima[63]. Gli attacchi cibernetici più sofisticati, realizzati talvolta attraverso l'uso di c.d. "armi cibernetiche", sono addirittura in grado di provocare la potenziale perdita di vite umane.

Alle molteplici finalità che possono essere perseguite da ciascun attacco cibernetico, riconducibili alle quattro macro-categorie di minacce già esaminate, si aggiunge l'intento dimostrativo, volto a creare un danno d'immagine in coincidenza di periodi di crisi o di tensioni sociali o politiche, quale aspetto tipico degli attacchi ideologicamente motivati, riferibili all'*hacktivism* [64].

Gran parte degli attacchi vengono perpetrati attraverso l' uso delle tecniche di *social engineering*, volte a manipolare, ingannare o semplicemente influenzare la mente umana, al fine di ottenere informazioni riservate o sensibili; è infatti l'essere umano, e non direttamente il sistema informatico o telematico, la vittima prediletta degli attacchi di ingegneria sociale, ossia di quelle tecniche fondate su processi cognitivi che approfittano dell'ingenuità del soggetto attaccato, per fini illeciti[65].

Si tratta di tecniche basate su abilità di natura psicologica e sociale che ricorrono alla capacità di ottenere la fiducia altrui attraverso lo studio dei

---

[62] *Ivi*, 27.

[63] V. FLOR, Cybersecurity *ed il contrasto ai* cyber-attacks *a livello europeo*, cit., 454.

[64] In argomento PRESIDENZA DEL CONSIGLIO DEI MINISTRI, *Quadro strategico nazionale per la sicurezza dello spazio cibernetico*, cit., 14 s.

[65] CAPONE, *Gli attacchi di ingegneria sociale*, in *www.cyberlaws.it*, 8 marzo 2018.

comportamenti in rete della vittima. L'utilizzo di queste tecniche psicologiche è finalizzato ad ingannare l'utente per indurlo a rivelare dati o informazioni personali, approfittando – come di è detto – dell'attitudine umana a riporre la fiducia negli altri[66].

Generalmente l'attaccante non è un singolo ma, sempre più spesso, si tratta di organizzazioni criminali che sfruttano la rete per ottenere profitto.

Non di rado l'attaccante crea la condizione per cui si trova a dover aiutare la vittima, quale ottimo metodo per instaurare o fortificare un rapporto di fiducia con il soggetto attaccato, il quale, di conseguenza, viene indotto ad essergli contestualmente grato ed obbligato: si determinano così attacchi di *sabotage*, *advertising and assisting*, denominati *reverse social engineering attacks*. Altre volte il soggetto attaccante si finge un'Autorità o un soggetto di rilievo per intimidire o creare un rapporto di dipendenza con la vittima.

L'ingegnere sociale, rientrante nella categoria degli *hacker*, è un soggetto istruito, esperto di informatica e psicologia, che agisce con premeditazione, previo studio dell'individuo da colpire, per conseguire profitti economici o vantaggi di altro genere. La scelta della vittima viene effettuata dall'*hacker* in base a diverse informazioni di natura psicologica ed economica, nonché in relazione al tipo di attacco che si intende sferrare.

Si è soliti distinguere, negli attacchi che si servono di tecniche di *social engineering*, quattro fasi principali: la prima, denominata *footprinting*, si riferisce al momento di preparazione, protraibile per un periodo medio-lungo in base alla difficoltà dell'attacco, e dedicato allo studio delle modalità più idonee all'approccio della potenziale vittima e al recupero delle informazioni; nella seconda fase, detta di "contatto", l'*hacker* inizia ad instaurare un rapporto con la vittima individuata, conquistando la sua fiducia; la terza è quella della "manipolazione psicologica", fase in cui si concretizza l'attacco, in cui l'ingegnere sociale cerca di carpire le informazioni riservate manipolando la vittima, per mezzo dell'utilizzo di tecniche psicologiche e strumenti per influenzarla; la quarta e ultima fase prevede la fuga,

[66] CUOMO, RAZZANTE, *La disciplina dei reati informatici*, Torino, 2007, 21.

poiché una volta concluso l'attacco, l'*hacker*, soddisfatto del risultato ottenuto, si distanzia dal contesto in cui ha operato, facendo perdere ogni sua traccia[67].

Quello dei *cyberattacks* è un fenomeno in continua crescita che, secondo quanto emerge dal rapporto CLUSIT 2020, ha vantato una diffusione incontrollata nel 2019, anno in cui si è registrato un esponenziale incremento, qualitativamente e quantitativamente, di attacchi cibernetici rispetto agli anni precedenti, con conseguente aumento della gravità dei relativi danni.

Il suddetto rapporto, inoltre, evidenzia come la maggior parte degli attacchi vengono realizzati con la finalità di commettere crimini cibernetici, e che le tecniche di attacco più utilizzate risultano essere quelle appartenenti alla categoria dei *malware*, a quella del *phishing* e degli attacchi d'ingegneria sociale in generale, e, in ultima analisi, a quella del *distributed denial of service*. Dal rapporto risultano però anche una serie di attacchi non appartenenti ad alcuna specie identificata, poiché, considerato il celere mutamento delle forme di aggressione, trattasi di tecniche sconosciute, ragion per cui vengono ricondotte nel gruppo *unknown*.

Ai numeri emersi dal rapporto vanno sommati tutti quegli attacchi di cui non è stata presentata denuncia, e che, in quanto tali, costituiscono le c.d. cifre nere, le quali compromettono l'elaborazione di uno studio completo in materia[68].

Anche il Report IOCTA 2019[69], predisposto dal Centro Europeo per la lotta alla criminalità informatica (EC3)[70], enfatizza la necessità di contrastare i suddetti attacchi attraverso la cooperazione nazionale e sovranazionale, pubblica e privata. È altresì fondamentale, nell' ottica preventiva, non solo adottare alcune contromisure, come *software antivirus* o *firewall*, ma anche incrementare la divulgazione della cultura informatica e della funzionalità di queste tecniche fra gli utenti, affinché la prevenzione possa dirsi efficace, poiché essa è tale solo laddove vi sia la consapevolezza della pericolosità delle minacce cibernetiche.

---

[67] Cfr. CAPONE, *Gli attacchi di ingegneria sociale*, cit.

[68] Per vedere le percentuali in merito, v. Rapporto CLUSIT 2020; in argomento anche *www.zerounoweb.it*. Un'alta percentuale degli attacchi realizzati nel primo semestre del 2020, come evidenziato dal Rapporto Clusit, è riconducibile alla situazione pandemica causata dal COVID 19 di cui il mondo è, ed è stato, vittima a partire dalla fine del 2019.

[69] *Internet Organized Crime Threat Assessment.*

[70] *European Cybercrime Centre (EC3), Europol*.

Anche se non esiste una contromisura infallibile, l'installazione del *software antivirus* rappresenta una delle più valide ed efficienti misure di difesa adottabili, poiché consente di isolare le forme di potenziale contaminazione, ossia il *software* maligno, prima che infettino altri dati.

La tecnica maggiormente impiegata per la rilevazione e l'eliminazione del *virus* consiste nella «scansione della memoria e delle unità a disco all'interno delle quali, se vengono rintracciate specifiche sequenze di *byte*, può affermarsi che il sistema è infetto e deve essere bonificato»[71]. Successivamente l'*antivirus*, dopo aver rilevato le sequenze di riconoscimento di un file infetto, segnala all'utente la presenza dell'intruso e tenta di neutralizzarlo, "ripulendo" il sistema, riducendo così il rischio di propagazione degli attacchi; occorre, inoltre, tenere il programma sempre aggiornato, affinché possa essere in grado di riconoscere e neutralizzare anche le nuove forme di contagio, in continuo cambiamento[72].

Gli attacchi moderni sono strutturati ed estremamente elaborati, inoltre molti di essi non si limitano a contaminare un solo computer, ma sono soliti diffondersi, con finalità distruttive o di disturbo, in ogni ambiente connesso in rete, provocando delle vere e proprie epidemie elettroniche o cibernetiche. Questi *software* interferiscono con le normali operazioni dei computer, giungendo, spesso, a danneggiare dati e programmi e addirittura, in alcuni casi, anche l'*hardware*[73].

Va però precisato che i principali mezzi di contagio, provenienti dall'esterno, si ravvisano non solo nelle reti di connessione internet, ma anche in tutti quei dispositivi di inserimento di nuovi dati o programmi, come ad esempio *floppy disk* o chiavi *USB*. Generalmente si tratta di programmi, generati da un programmatore, autonomi o dipendenti da altri *softwar*e, che si attivano e si propagano, alcuni dei quali creando copie di sé stessi, indipendentemente dalla volontà dell'utente, prendendo il controllo di quante più possibili funzioni del sistema operativo. Si noti altresì che alcuni attacchi producono danni immediatamente, mentre altri rimangono in pausa fino a che non vengono attivati inconsapevolmente dagli utenti[74].

---

[71] V. CUOMO, RAZZANTE, *La disciplina dei reati informatici*, cit.,132.
[72] *Ivi*, 131.
[73] Cfr. SARZANA DI S. IPPOLITO, *Informatica, Internet e diritto penale,* cit., 95.
[74] Sul punto CUOMO, RAZZANTE, *La disciplina dei reati informatici*, cit., 123 ss.

Per ciò che concerne la sicurezza delle infrastrutture assume rilevanza anche il *firewall*, quale dispositivo per la sicurezza della rete che funziona come se fosse un filtro, evitando connessioni a rischio per il sistema; esistono, inoltre, vari tipi di *firewall* a seconda che la rete da difendere sia più o meno estesa.

In linea di massima un attacco può suddividersi nelle seguenti fasi: una prima fase di studio del sistema bersaglio e delle relative criticità; una fase successiva di accesso; un'ultima fase concernente la presa del controllo del computer[75].

Dagli attacchi cibernetici derivano molteplici conseguenze dannose che colpiscono specialmente e più severamente le aziende, tra le quali la più evidente è sicuramente la ripercussione economica che può essere causata dall'interruzione o dal malfunzionamento del sistema, dall'immediata sospensione delle attività e dalla perdita di informazioni sensibili o finanziarie dovute al pregiudizio subito dai file, dalle risorse economiche e dai tempi utili per la bonifica ed il ripristino della normale operatività del sistema, oltreché dal pagamento di un possibile riscatto richiesto dall' *hacker*.

Le ulteriori conseguenze contemplano danni di natura reputazionale, a causa della lesione all'immagine per non aver protetto adeguatamente il sistema con le apposite misure, danni di natura legale, a seguito dell'insorgere della responsabilità contrattuale o extracontrattuale derivante dalla perdita dei dati o dall'inadempienza dovuta all'interruzione dell'attività, o danni di natura sanzionatoria, per via della conseguente applicazione delle sanzioni espressamente contemplate[76].

Tra i principali attacchi informatici ve ne sono alcuni, il cui esame è funzionale alla più ampia conoscenza del fenomeno, nonché alla completezza della trattazione, costituendo essi, tra l'altro, alcuni degli strumenti di commissione dei *cybercrimes*.

Il *malware*[77] rappresenta una tipica tecnica di attacco cibernetico semplice, vale a dire consistente in una sola operazione; è un *software* malevolo, ossia un

---

[75] *Ivi*, 18.

[76] V. PANATTONI, Compliance, cybersecurity *e sicurezza*, cit., 29.

[77] V. MEZZALAMA, LIOY, METWALLEY, *Anatomia del* malware, in *Riv. Mondo Digitale*, 2013, 47, 2: il termine *malware* discende dall' unione delle parole *malicious* e *software*, letteralmente programma dannoso.

programma capace di colpire sistemi, dispositivi mobili e reti, ostacolando la regolare funzionalità del computer. È progettato per accedere ad un sistema informatico, senza il consenso dell'utente, al fine danneggiarlo o per sottrarre dati sensibili o spiare le vittime.

Vi sono varie categorie di *malware*, ciascuna delle quali utilizza tecniche, strumenti e strategie distinte, ma con un modello strutturale di base unico, che si fonda sulle quattro fasi di seguito riportate: la prima riguarda l'infezione, e cioè il momento in cui il *software* malevolo s'inserisce nel sistema oltrepassando le possibili barriere di sicurezza, e s'insedia al suo interno modificando le impostazioni del sistema per restare nascosto; la fase successiva è quella della quiescenza, in cui il *malware* si trattiene silente in memoria in attesa di essere avviato, confondendosi con gli altri programmi archiviati, e tale momento si proroga fino all'eliminazione autonoma o dovuta ad un apposito *software anti-malware*; la terza fase corrisponde alla replicazione e alla propagazione, per cui il *malware*, a determinate condizioni, identifica nuovi *target* e riproduce se stesso al fine di infettarli; la quarta e ultima fase prevede la realizzazione di azioni malevole, consistenti nella distruzione o nel furto dei dati o dei sistemi, e se non si verificano le suddette operazioni di compromissione definitiva, il *malware* torna nella fase due, cioè quella della quiescenza.

L'introduzione del *software* malevolo all'interno del sistema identificato può avvenire attraverso tre diversi canali, il primo dei quali si ravvisa nel trasferimento fisico del *malware* dal supporto di memorizzazione al sistema stesso. Altro canale di trasmissione è rappresentato dalla posta elettronica, in quanto il codice malevolo non di rado viene incluso nei messaggi inviati all'utente, il quale, persuaso dalle tecniche di *social engineering*, è indotto ad aprire l'allegato contenente il *malware*. Per giunta il *software* malevolo può essere diffuso anche per mezzo di un *download* dal *web*, effettuato inconsapevolmente dall' utente. Gli ultimi due canali rappresentano, ad oggi, la modalità di trasmissione più comune.

Si tratta di un codice malevolo che, una volta introdottosi nel sistema, deve essere attivato, ragion per cui non solo è spesso richiesta la cooperazione della

vittima, ma il *malware* deve anche apparire come il più innocuo possibile, assumendo l'aspetto di un contenuto lecito[78].

Nella macro-categoria dei *malware* si è soliti ricomprendere *virus, worm, trojan horse, spyware, adware, keylogger e ramsomware.*

Il *virus* non è un *software* autonomo, poiché per attivarsi è richiesta l'esecuzione del programma che lo ospita, il quale a sua volta diviene contagioso; si tratta di un *software* capace di infettare *file* e programmi al fine di danneggiare sistemi, cancellare dati, aprire *blackdoor*, cambiare l'aspetto di un video, disabilitare i *software antivirus*, e più in generale di compromettere il normale funzionamento del computer. Questo tipo di codice malevolo passa da un sistema all'altro, e in ciascuno di essi lavora indipendentemente dal *virus* iniziale, poiché capace di riprodursi in altri luoghi senza essere notato dall'utente[79].

Il *worm* è un programma dotato di autonomia, che non necessita né di un programma ospite in cui insediarsi, né della cooperazione dell'utente. È solito diffondersi, per mezzo di una rete, su vari computer, infettandoli fino alla saturazione dei sistemi, seppur non compromettendo i *file* presenti.

Tali software sono stati realizzati per bloccare le reti di trasmissione, riconoscendogli una rapida ed estesa capacità di diffusione, agevolata dall' impiego di programmi di posta elettronica attraverso i quali il *worm* circola, inviando una sua copia a tutti i contatti, identificati quali possibili nuovi bersagli[80].

Un ulteriore veicolo di diffusione può ravvisarsi nelle memorie di massa come *pen drive* o *hard disk*. In questo caso «il segmento ricostruito del programma si mantiene in comunicazione con il segmento dal quale deriva»[81]. Tra i *worm* più conosciuti vi è *Confiker*, scoperto nel 2008, il quale, sfruttando un difetto di rete del sistema, ha infettato milioni di piattaforme Microsoft Windows.

Il *trojan horse* si mostra all'utente come un programma apparentemente utile, ma al suo interno nasconde funzionalità malevole; si tratta infatti di «una

[78] Sul punto MEZZALAMA, LIOY, METWALLEY, *Anatomia*, cit., 2 ss.; PANATTONI, Compliance, cybersecurity *e sicurezza*, cit., 26.

[79] In argomento CUOMO, RAZZANTE, *La disciplina dei reati informatici*, cit., 22; SARZANA DI S. IPPOLITO, *Informatica, Internet e diritto penale,* cit., 93 s.

[80] V. CUOMO, RAZZANTE, *La disciplina dei reati informatici*, cit., 129.

[81] SARZANA DI S. IPPOLITO, *Informatica, Internet e diritto penale,* cit., 94.

sezione di codice nascosto in un programma legittimo»[82] che si introduce subdolamente e innocuamente all'apparenza, e che può essere attivato all'istante o può continuare ad operare regolarmente per un periodo di tempo prima di attivarsi. È un *software* incapace di replicarsi, ed è volto ad eseguire funzioni non autorizzate o a bloccare il funzionamento del computer; esso è altresì considerato autonomo, poiché non ha bisogno di compromettere altri *file* per raggiungere il suo obiettivo; non si autopropaga ad altri computer, ma deve essere inviato direttamente macchina per macchina, infettando solo i riceventi prescelti.

Generalmente, il "cavallo di Troia" viene utilizzato da chi vuole introdursi, senza il consenso dell'utente, in un sistema informatico per mezzo di Internet, al fine di controllarlo da remoto, servendosi frequentemente di *"blackdoor"*, grazie ad un altro computer che attiva il *software*[83]. Inoltre, questo programma è così sofisticato che è in grado di prendere visione dello schermo e di attivare *webcam* e microfoni.

Il *trojan horse* si sostanzia di due *file* tra loro complementari, il *file client*, attraverso cui avviene il controllo, e il *file server*, che è insidiato nel *computer* bersaglio e svolge i comandi ricevuti dal *file client*[84].

Esiste tuttavia un particolare tipo di *trojan*, definito "*trojan* di Stato" o più comunemente "captatore informatico", che viene impiegato lecitamente, seppur a determinate condizioni ed entro certi limiti, al fine di svolgere attività investigativa con riguardo a delitti di particolare gravità, tra i quali quelli di criminalità organizzata o contro la pubblica amministrazione, come appositamente previsto dalla disciplina oggetto del d.lgs. n. 216/2017, attuativo della Legge delega n. 103/2017, meglio conosciuta come Legge Orlando[85].

Si tratta di un mezzo di ricerca della prova che ha profondamente rivoluzionato e agevolato, anche se in ambiti circoscritti, il tradizionale svolgimento

---

[82] *Ibidem*.

[83] In argomento CUOMO, RAZZANTE, *La disciplina dei reati informatici*, cit., 128; SARZANA DI S. IPPOLITO, *Informatica, Internet e diritto penale,* cit., 94.

[84] V. SILVETTI, *I crimini informatici più frequenti degli ultimi anni: tabella riepilogativa e profili giuridici*, in *Quot. giur.*, 4 ottobre 2019.

[85] GIORDANO, *Presupposti e limiti all'utilizzo del captatore informatico: le indicazioni della Suprema Corte*, in *Sist. Pen*, 2020, 4, 109 ss.

delle indagini ad opera degli inquirenti, potendo ora attingere, in tale fase, ad uno strumento innovativo, seppur estremamente invasivo[86].

Una delle più recenti forme di *trojan* scoperte è il *trojan Ginp*, un *mobile banking trojan* che, approfittando della situazione pandemica mondiale causata dal *virus* SARS-CoV-2 (c.d. "Covid-19"), viene introdotto negli *smartphone* delle vittime per mezzo dell'installazione di un'applicazione, la quale promette di individuare quanti più soggetti contagiati nelle vicinanze in cambio del pagamento di una piccola somma di denaro; tuttavia, l'addebito in questione non viene effettuato, poiché il fine ultimo di questo attacco è quello di ottenere le credenziali della carta di credito dell'utente[87].

Per altro verso, viene in rilievo lo *spyware*, ovverosia un *software* utilizzato per prelevare, senza autorizzazione, dati sensibili dal sistema in cui è occultamente inserito, rappresentando una minaccia alla sicurezza della *privacy*; successivamente le informazioni riservate vengono trasmesse al *server* remoto del destinatario interessato ad ottenerle fraudolentemente, il quale le impiegherà per ricavare profitto ovvero progettare attacchi informatici *ad personam*, producendo ad esempio. pubblicità mirata in base alle preferenze della vittima.

Anche questa tipologia di *malware* può essere impiegata, secondo quanto previsto dal d.lgs. n. 216/2017, per effettuare intercettazioni di discorsi o comunicazioni in dispositivi mobili.

Solitamente lo *spyware* viene inserito nel computer bersaglio facendo uso delle tecniche di *social engineering,* le quali sorvegliano e tracciano le abitudini degli utenti[88]. Alcuni dei più importanti vettori di contagio sono i *cookies*, *link,* allegati e pubblicità ingannevole[89].

---

[86] Per approfondire sul punto v. SENOR, *Come funzionano i* trojan *di stato? Analisi delle nuove norme e indicazioni operative, in* www.altalex.com, 22 gennaio 2018.

[87] Cfr. Rapporto Clusit 2020, *Speciale pandemia*, 77 ss.; TARSITANO, Ginp, *il* trojan Android *che finge di segnalare i contagiati da Coronavirus*, in *www.cybersecurity360.it,* 25 marzo 2020.

[88] V. LOMBARDO, Spyware*: cosa sono, come si diffondono e come eliminarli, in www.cybersecurity360.it,* 16 Maggio 2019.

[89] Cfr. *Ibidem*: «**I cookies**: sono delle informazioni di sessione (dati di navigazione) che usualmente i siti Web memorizzano sui computer dei client. Questi dati possono essere rubati ed utilizzati per accessi impersonificati; **l*ink* e allegati**: sfruttando le vulnerabilità nella sicurezza dei *browser* è sufficiente cliccare su di un l*ink*, un allegato di una e-mail per avviare uno script e dirottare la vittima, in modo inconsapevole, verso un sito *Web* per il download di codice malevolo (***drive by* download**); **pubblicità ingannevole**: gli attaccanti possono ingannare gli utenti, invitandoli a

Ancora, l'*adware* è un programma progettato per proiettare annunci pubblicitari indesiderati, dirottare le richieste degli utenti verso siti *web* promozionali e acquisire dati di *marketing*, al fine di trasmetterli a server remoti, facendo così intuire la finalità prettamente commerciale di questo tipo di *software*.

Il *keylogger* è capace di registrare qualunque *input* derivante dalla tastiera, e, quindi, di captare tutto ciò che l'utente digita, dalle informazioni più inutili a quelle più rilevanti, come ad esempio le chiavi d'accesso. Vi sono due tipi di *keylogger*, quello *hardware*, che richiede l'inserimento di un dispositivo elettronico all'interno della tastiera, necessitando di un contatto tra la stessa e la vittima, e quello *software*, costituito semplicemente da un programma informatico capace di cogliere qualunque *input*[90].

Il *ransomware* è un *malware* di tipo estorsivo, il cui termine «deriva dalla crasi delle parole inglesi *malware* (programma malevolo) e *ransom* (riscatto)»[91] e, in base alla tipologia, questo può «cifrare, occultare o negare l'accesso a dati o informazioni, oppure limitare o impedire l'accesso al sistema informatico, al fine di costringere la persona offesa a versare un importo per lo "sblocco"»[92]. In altri termini, quindi, si tratta di un *malware* che mira ad infettare un computer, bloccandone l'utilizzo per mezzo della criptazione dei *file* memorizzati *sull'hard drive,* o impedendo l'accesso al dispositivo stesso, e per il cui ripristino viene presentata una richiesta di riscatto da corrispondere su conti bancari anonimi o per mezzo di criptovalute[93].

Questa tipologia di attacco sembrerebbe articolarsi in una condotta bifasica, poiché in un primo momento si ravvisa un attacco informatico e successivamente una minaccia telematica con richiesta di riscatto, da versare in termini perentori per il recupero dei dati[94].

---

scaricare e installare un programma, presentando e camuffando lo *spyware* come un indispensabile strumento di utilità. Spesso queste utility pur disinstallandole possono lasciare persistenti e funzionanti le proprie componenti malevole».

[90] Sul punto RIJTANO, Keylogger: *cos'è, come eliminarlo, i migliori per Windows, Mac e cellulare, in* www.cybersecurity360.it, 24 maggio 2018.

[91] Cfr. LUBERTO, *"Sex-Torsion" via web e minaccia a mezzo* ransomware*: la nuova frontiera del delitto di estorsione*, in CADOPPI, CANESTRARI, MANNA, PAPA (diretto da), Cybercrime. Torino, 2019, 729.

[92] *Ibidem*.

[93] In argomento PANATTONI, Compliance, cybersecurity *e sicurezza*, cit., 27.

[94] V. LUBERTO, "Sex-Torsion*" via web e minaccia a mezzo* ransomware, cit., 729.

Generalmente, dopo aver corrisposto la cifra oggetto di riscatto, all'utente viene inviata una *e-mail* contenete le istruzioni per avviare un *download* di decriptazione, anche se spesso costui, dopo aver effettuato il pagamento, potrebbe trovarsi nella condizione di irrecuperabilità di alcuni *file*, poiché cancellati definitivamente dal *ransomware,* o nell' impossibilità di accedere nuovamente al sistema.

Nell'ambito di tale attacco, il *bitcoin* è la moneta virtuale più richiesta, in ragione della non tracciabilità auspicata dal *cyber*-criminale. È una valuta nascosta che si scambia solo telematicamente, ed è visibile esclusivamente da chi possiede uno specifico codice informatico; la transazione, invece, sarà rilevabile dal sistema *blockchain*[95].

Il più delle volte questo tipo di *malware* si introduce nel sistema tramite *download* da Internet, o più semplicemente sfruttando le debolezze del servizio di rete, anche se il mezzo più frequente resta la posta elettronica, poiché gli utenti traditi dagli indirizzi *e-mail* noti, sono indotti ad aprire e scaricare gli allegati, attivando così il *malware* estorsivo.

Tra gli aspetti più rilevanti tipici di questo tipo di attacco figura non solo il pregiudizio che colpisce, come in tutti gli altri casi, la sicurezza informatica, ma anche quello che inficia la riservatezza, la confidenzialità e la libertà delle informazioni, e quindi più in generale la *privacy*.

Attualmente è la categoria di *malware* più diffusa, e, negli ultimi anni, tale software ha contagiato migliaia di computer appartenenti ad enti pubblici e società private, causando immensi danni economici. Tra gli esempi più devastanti vi sono *Cryptolocker* e *Wannacry*.

Cryptolocker appare per la prima volta nel 2013 e successivamente nel 2017: è un *software* malevolo che ha compromesso moltissimi sistemi *Windows*, criptando i dati in esso archiviati e chiedendo il pagamento di un riscatto. Esso è solito diffondersi come allegato di posta elettronica o mediante un computer ricompreso in una *botnet*[96]. L' allegato si presenta come un *file zip* contenente un

[95] Per approfondire sul punto v. CONSOB, *Le criptovalute: che cosa sono e quali rischi si corrono*, in www.consob.it.

[96] V. RIJTANO, Cryptolocker*, cos'è, come si prende e come difendersi*, in *www.cybersecurity360.it*, 2 luglio 2018: si tratta di reti costituite da computer, controllate da un

f*ile* eseguibile con estensione pdf, che una volta avviato consente al *software* di installarsi e di connettersi ad uno dei *server* di comando, di difficile tracciabilità, il quale genera una chiave "RSA", inviando la chiave pubblica al computer contaminato. A seguire, il *malware* cifra i *file* dell'*hard disk* e delle condivisioni di rete per mezzo della chiave pubblica, e comunica all'utente l'avvenuta criptazione e la richiesta di riscatto che, se non viene corrisposto nei termini, determinerà l'eliminazione della chiave privata funzionale alla decriptazione dei *file*, divenendo così irrecuperabili.

Quanto invece a *Wannacry*, questo è un *malware ransomware* che nel 2017 ha infettato oltre duecentomila computer, colpendo paesi di tutto il mondo. Benché sia innegabile il danno economico dovuto al pagamento dei riscatti, la cifra incassata si aggira intorno ai 100 mila dollari, facendo presumere che l'attacco non sia stato sferrato per soldi ma quasi certamente con fini dimostrativi o destabilizzanti.

Più precisamente, si tratta di un *crypto-ransomware* che cifra i *file* dei computer collegati alla rete e con sistema operativo *Windows*, rendendoli inaccessibili e chiedendo un riscatto da pagare in cambio della decriptazione. La propagazione del *software* avviene tramite posta elettronica o chiavette USB, o mediante *exploit*, attraverso il protocollo "SMB", vale a dire *Server Message Block*, in computer non aggiornati, automaticamente, sfruttando le condivisioni di rete.

È un *malware* costituito da due componenti che operano in sequenza: un *expolit*, che approfitta delle debolezze del sistema per colpire il computer bersaglio; un *ramsomware* vero e proprio, funzionale alla criptatura dei *file* e alla relativa richiesta di riscatto per la decriptazione. Nel 2017 sono stati contagiati specialmente enti pubblici ed ospedali, i quali non avevano aggiornato i sistemi che li avrebbe resi immuni dall'attacco[97].

amministratore che si serve di esse per sferrare attacchi simultaneamente, «le *botnet* sono nate come reti di elaboratori usati per gestire e mantenere attivi servizi *Web*. I *criminal hacker* le hanno trasformate in reti di computer compromessi da usare per eseguire attività fraudolente».

[97] Per approfondire sul punto v. DAL CHECCO, Il ransomware Wannacry *infetta PC non aggiornati: ospedali ed enti pubblici a rischio*, in *www.ransomware.it*, 12 maggio 2017; RIJTANO, SBARAGLIA, *WannaCry, cos'è, come funziona e come difendersi dal ransomware che ha fatto piangere il mondo*, in *www.cybersecurity360.it*, 28 giugno 2018.

Al fine di contrastare simili attacchi estorsivi è opportuno adottare idonee misure di prevenzione e tecniche difensive all'avanguardia, basate su una corretta analisi del rischio volta a selezionare i *software* in pericolo; in particolare, il suddetto obiettivo viene perseguito mediante il costante aggiornamento dei sistemi operativi, per mezzo della predisposizione di sistemi *antivirus* moderni, realizzando frequenti *backup* e mostrando maggiore attenzione nei confronti di allegati di posta elettronica inaspettati.

Ad ogni modo è preferibile non pagare il riscatto, poiché spesso ciò non è garanzia del ripristino dei *file*, che, al contrario, può avvenire facendo uso dei programmi di decriptazione, ideati dai produttori degli *antivirus*[98], applicabili autonomamente e gratuitamente, ma che spesso a causa della più veloce evoluzione del *malware* rischiano di essere insufficienti.

Tra gli attacchi cibernetici semplici rientrano anche *il Man in the middle*, il *Denial of service, il DNS poisoning* e lo *spam*. Quest'ultimo[99] consiste nell'invio incessante, e senza consenso, di posta indesiderata, costituita principalmente da pubblicità spazzatura o contenente siti malevoli a cui gli utenti sono indotti a connettersi, tramite *e-mail*, *chat* e *post social*.

Lo spam rappresenta uno dei maggiori veicoli per la diffusione dei *malware*, poiché è in grado di raggiungere milioni di computer, concorrendo ad accrescere il traffico sulla rete internet.

L'aspetto che più interessa ai fini della trattazione è ravvisabile nel fatto che, negli anni, l'invio di messaggi pubblicitari di massa ha acquisito un risvolto molto

---

[98] Per approfondimenti sul punto v. SANTORO, *Il progetto internazionale "*No more ransom" *alla luce dell'attacco* WannaCry, in *Quot. giur.* Web&Tech *Sicurezza informatica*, 1° giugno 2017: al fine di sensibilizzare gli utenti ed educarli all' autonoma decriptazione dei dati compromessi, il progetto "*No more ransom*", predisposto da un' intesa internazionale, a cui hanno partecipato pubblici e privati, tra cui *kaspersky* e l' *European cybercrime centre* dell' *Europol*, individua i mezzi di recupero alternativi al pagamento del riscatto, incitando gli utenti a recuperare i file in autonomia, scoraggiandoli dall'alimentare una politica cybercriminale.

[99] Cfr. PIVATO, Lo spam*: cos'è e come difendersi, anche alla luce del GDPR,2019,* in *www.cybersecurity 360.it*, 13 novembre 2019: «Il termine *spam*, nasce quale conseguenza di uno sketch comico del *Monty Python's Flying Circus,* famosa serie TV britannica degli Anni 70, nel quale una cameriera illustrava il menu composto da sole pietanze a base di s*pam*, una famosa carne in scatola diffusa in Inghilterra durante la Seconda guerra mondiale (e immediatamente identificata come *junk food*, cioè cibo spazzatura). Questa gag ebbe così tanto successo che **il termine *spam* fu associato a qualcosa d'inevitabile e onnipresente** e appunto, alcuni anni dopo, al **fenomeno dell'invio, senza consenso, di comunicazioni ai fini di marketing** (pubblicità, indagini di mercato, comunicazioni commerciali), effettuato attraverso l'utilizzo di sistemi automatizzati».

rischioso, poiché, ad oggi, può, in alcuni casi, essere vettore per l'*e-mail* di *phishing* e veicolare truffe informatiche[100].

Ultimamente si sta diffondendo una nuova tipologia di *spam* basata sulla comunicazione virale, ossia la capacità comunicativa di trasmettere un messaggio a moltissimi utenti, facendo uso di sistemi automatizzati e incentivando l'inoltro del messaggio grazie alla prospettiva di ricevere dei premi o delle ricompense.

Inoltre, è opportuno precisare che secondo quanto disposto dal GDPR, e dall'art. 130, co.1, del Codice della Privacy, come modificato dal d.lgs. n. 101/2018, la pratica dello *spam* è vietata, a meno che non vi sia il consenso preventivo dell'utente, quale requisito fondamentale per poter inoltrare avvisi pubblicitari per mezzo di sistemi automatizzati[101].

Nel tempo le tecniche di aggressione sono notevolmente migliorate, sviluppandosi *cyberattacks* complessi, composti da molteplici operazioni tra loro connesse, e tra i quali figurano il *phishing*, il *pharming*, la *botnet*, il *distributed denial of service* e il *watering hole.*

Gran parte degli autori degli attacchi informatici è costituita da soggetti genericamente definiti "*hacker*s"[102], i quali rappresentano il semplice e naturale prodotto della rivoluzione tecnologica e della civiltà digitale[103].

Attualmente la categoria degli *hackers* ricomprende soggetti che, solitamente, sfruttano le loro elevate conoscenze e competenze tecnologiche per aggredire i sistemi informatici e telematici.

---

[100] Tali condotte delittuose saranno esaminate *infra* Cap 2, § 2.2, 2.3, Cap 3, § 3.2.

[101] Cfr. PIVATO, Lo spam, cit.: «Alla luce del GDPR e dell'art. 130, comma 1, del Codice *Privacy* come modificato dal D.lgs. 101/2018 **la pratica dello *spam* è vietata**. Infatti, l'uso di sistemi automatizzati d'invio di materiale pubblicitario, di vendita diretta, di comunicazione commerciale o per il compimento di ricerche di mercato **è possibile solo se sussiste il consenso preventivo dell'utente** (cosiddetto ***opt-in*)**. Pertanto, in assenza di detto consenso è illegittimo l'invio di comunicazioni promozionali con i predetti strumenti. Quindi, **il consenso è un requisito cardine per poter inviare comunicazioni pubblicitarie attraverso sistemi automatizzati** e l'art. 4 del GDPR lo definisce come la manifestazione di volontà libera, specifica, informata ed inequivocabile dell'interessato».

[102] In argomento v. CUOMO, RAZZANTE, *La disciplina dei reati informatici*, cit., 16: «Il termine "hacker" nella sua accezione originaria (dall' inglese " *to hack*" che letteralmente significa " fare a pezzi" o " tagliare"), indica una persona per la quale la programmazione informatica costituisce una vera e propria passione , con l'obiettivo di dominare le macchine, di smontare i sistemi, di osservare come sono costruiti e come funzionano per scoprirne peculiarità nascoste e debolezze, o per implementare ed innovare le applicazioni».

[103] In argomento SARZANA DI S. IPPOLITO, *Informatica, Internet e diritto penale,* cit., 84.

La "cultura *hacker*"[104] si è diffusa per la prima volta tra docenti e studiosi di informatica, alla fine degli anni Cinquanta, al "*Massachusetts Institute of Technology*" di Cambridge, epoca ed ambiente in cui gli *hacker* erano ritenuti personaggi che lavoravano sui sistemi informatici e intendevano confrontarsi con le macchine proprio al fine di dar prova di innovazione e abilità tecnica. Solo in un secondo momento, con la diffusione di Internet e delle più evolute tecnologie, le tecniche di *hacking* sono state utilizzate per scopi illeciti e intenti criminosi, mutando irreversibilmente l'originaria accezione del termine *hacker* e attribuendogli una connotazione decisamente dispregiativa, identificativa del c.d. "pirata informatico". Più precisamente, ad oggi, l'espressione *hacker* viene utilizzata globalmente per indicare tutti quei soggetti il cui comportamento integra una fattispecie di reato informatico o cibernetico[105].

Questa categoria di soggetti costituisce motivo di allarme sociale, in ragione della significativa rilevanza collettiva che assumono le intrusioni informatiche e i sabotaggi da esse realizzati.

In base al *modus operandi*, alla condotta e all'abilità tecnica si possono distinguere diverse tipologie di *hackers*, non essendo questa una categoria uniforme. Alcuni esperti, considerato il diverso livello di abilità, differenziano tre figure di *hackers*: la prima è quella dei *crackers*, ossia professionisti di altissimo livello, con elevate competenze tecniche e ampia esperienza; la seconda concerne gli *hacker* veri e propri, quali tecnici di medio livello e conoscenza; l'ultima figura è quella relativa ai *rodents*, soggetti di basso profilo tecnico[106].

Altri specialisti in materia, a seconda del tipo di comportamento adottato, individuano tre ulteriori e distinte classi di *hackers*: la prima classe è quella degli esperti veri e propri che «violano i sistemi mediante indagini sistematiche ed il loro obiettivo è quello di infrangere i sistemi di sicurezza e curiosare negli schedari, soddisfatti di aver raggiunto il loro scopo»[107]; la seconda comprende gli *swappers*, i

---

[104] Cfr. CUOMO, RAZZANTE, *La disciplina dei reati informatici*, cit., 17: «Secondo la "cultura *hacker*" i sistemi di elaborazione potevano essere violati per elevare il livello delle conoscenze scientifiche e per verificare l'efficacia delle protezioni contro le intrusioni, anche se non era consentito danneggiare i programmi e le informazioni».

[105] *Ivi*, 18.

[106] In argomento SARZANA DI S. IPPOLITO, *Informatica, Internet e diritto penale*, cit., 88 ss.

[107] *Ivi*, 89.

quali «rappresentano la grande maggioranza degli *hacker*. Sono dediti piuttosto allo scambio di informazioni e all'uso dei sistemi a scopo ludico, ai quali accedono attraverso informazioni ricevuti, piuttosto che in base ad indagini tecniche sistematiche: si limitano per lo più a curiosare»[108]; la terza classe è relativa ai vandali elettronici, i quali «rappresentano una minoranza nel campo degli hackers e spesso sono osteggiati dalla maggioranza degli "hackers buoni". Essi sono specializzati nel penetrare nei sistemi lasciandovi messaggi osceni o cancellando gli schedari o alterando il sistema di "passwords". Sono particolarmente vendicativi e molto inclini alle ritorsioni, anche gravi»[109].

1.2.2 Il passaggio dai *computer crimes* ai *cybercrimes*: le caratteristiche dei reati informatici e cibernetici.

Lo sviluppo tecnologico e la conseguente diffusione dell'informatica e della telematica, come osservato in precedenza, hanno determinato un profondo cambiamento sociale, trovando applicazione in qualunque settore della c.d. "società dell'informazione". I profili di vulnerabilità propri della tecnologia aumentano in corrispondenza dello sviluppo informatico, trattandosi di un settore complesso ma estremamente fragile. Questo tipo di rivoluzione ed i rischi ad essa connessi hanno provocato la contestuale comparsa di una nuova realtà delinquenziale, ricomprendente nuovi comportamenti dannosi, assimilabili solo in parte a quelli tradizionali, in virtù delle facilitazioni tecniche e delle distorsioni percettive proprie della dimensione digitale che influenzano l'*it*er criminoso[110].

Nel corso del tempo, la criminalità si è adeguata ai cambiamenti storici, sociali e tecnologici, stravolgendo la classica concezione di delinquenza e rivolgendosi a beni giudici inediti – da aggiungere a quelli tradizionali – ,anche e soprattutto in ragione delle tipicità proprie del *cyberspace*, ravvisabili nella smaterializzazione, nell'anonimato, nell'aterritorialità, e nell'atemporalità.

Nel concetto di criminalità informatica, non giuridicamente definito, sono ricomprese tutte quelle condotte antigiuridiche connesse all'utilizzo della

[108] *Ibidem*.
[109] *Ibidem*.
[110] In argomento BALLONI, BISI, SETTE, *Principi di criminologia applicata*, cit., 271.

tecnologia[111], che rappresentano una costante minaccia per i singoli e per la collettività; in particolare, nella società moderna, l'espressione "criminalità informatica" è impropriamente e comunemente utilizzata per indicare anche tutti quei fatti criminosi che possono essere realizzati attraverso la rete o nel *cyberspace*, attribuendo così una più ampia accezione al termine, che diviene, sempre più spesso, sinonimo di "criminalità cibernetica"[112]. Quest'ultima, inoltre, in virtù delle suesposte tipicità riconducibili al *cyberspace*, non può essere limitata ad un numero chiuso di reati, includendo, al contrario, una crescente molteplicità di illeciti, alcuni dei quali di nuova entità.

Le prime forme di criminalità informatica moderna, risalenti ai primi anni Settanta, e dovute a condotte antigiuridiche conseguenti all'impiego del *personal computer*, sono definite *computer crime*s o *computer-related crimes*, proprio a voler sottolineare l'elaboratore quale mezzo usato dal criminale. A questi reati informatici, «connessi solo eventualmente in reti telematiche chiuse o ad accesso circoscritto»[113], si riferiva il legislatore del '93, utilizzando, all'epoca, la locuzione "sistema informatico o telematico" per indicare l'insieme di singoli sistemi strutturati in più *client* con *server* e reti chiuse[114].

Il cambiamento epocale, risalente a metà degli anni '90 del Novecento, e ravvisabile nell'apertura di Internet[115] alla totalità degli utenti, ha trasformato la rete in una rete globale[116], accessibile e utilizzabile da chiunque. Questa significativa

---

[111] *Ivi*, 254.

[112] FLOR, *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di internet,* in *Dir. pen. cont.*, 20 settembre 2012, 4; cfr. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, cit., 51: «Di fronte alla nuova realtà è cambiato, dunque, di passo l'approccio alla criminalità informatica, a sua volta divenuta "criminalità cibernetica" o, meglio, criminalità "nel" *Cyberspace*».

[113] Cfr. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, cit., 47.

[114] *Ibidem*: «Al massimo si pensava a banche di dati private o pubbliche, accessibili "da remoto", qual era il famoso CED della Suprema Corte di Cassazione, antesignano di un'informatizzazione della giustizia italiana (percepita come indispensabile ed urgente da magistrati lungimiranti), che purtroppo ha poi segnato a lungo il passo; ovvero all'anagrafe tributaria, comunque ad accesso ristretto, od al CED del Ministero dell'Interno, istituito con la legge di riforma della Polizia di Stato del 1981[…]».

[115] Per approfondire la nascita e l'evoluzione di Internet in un mezzo di comunicazione massiva v. *voce Internet,* in *Enc. onl. Treccani*, consultabile su *www. treccani.it*.

[116] Cfr. BALLONI, BISI, SETTE, *Principi di criminologia applicata*, cit., 253: «Internet, in tal senso, non si pone più nei soli termini di strumento per facilitare le quotidiane operazioni di studio e lavoro, ma diviene una sorta di palcoscenico in cui gli utenti possono "mettere in scena" diverse dimensioni del proprio sé e in cui, al contempo, possono dar vita a relazioni effettive e potenziali

novità, su cui si fonda la nuova dimensione del *cyberspace*, ha determinato il mutamento della criminalità da informatica a cibernetica, segnando il passaggio dalla categoria dei *computer crimes*, o reati informatici, a quella dei *cybercrimes*, o reati cibernetici, sfruttando i nuovi spazi e le maggiori possibilità per compiere azioni non solo lecite ma anche di natura delinquenziale.

L'attuale epoca di internet, inoltre, sembrerebbe richiedere un costante adeguamento delle disposizioni in materia, coerentemente con le innovazioni del settore, poiché l'apertura di Internet alla collettività e le potenzialità proprie della rete hanno stimolato, agevolato e rafforzato il compimento di attacchi informatici, e la conseguente commissione di numerosi e diversificati illeciti in rete ovvero tramite la rete[117].

Sembra dunque opportuno intendere la "criminalità informatica", o più in generale "cibernetica", come un fenomeno elastico e ad ampio raggio, rispetto al quale è possibile effettuare una classificazione delle manifestazioni criminose, partendo dalla configurazione della categoria dei reati informatici – c.d. "in senso stretto" e "in senso ampio" – per giungere a quella più vasta e generale dei reati cibernetici – anch'essi, c.d. "in senso stretto" e "in senso ampio"[118]; questi differiscono dai reati tradizionali specialmente per il modo in cui sono realizzati.

I reati informatici "in senso stretto" si riferiscono alle fattispecie incriminatrici legislativamente formulate richiamando almeno un elemento che si riferisca esplicitamente ed inequivocabilmente alle tecnologie dell'informazione e della comunicazione, il quale deve tassativamente risultare integrato ai fini della sussistenza delle fattispecie suddette[119].

I reati informatici "in senso ampio", al contrario, sono tutti quelli che possono essere commessi anche attraverso strumenti informatici o ricadere altresì

---

all'interno di nuovi spazi che, sebbene siano "virtuali" nella loro natura, divengono "reali" nelle conseguenze che producono».

[117] In argomento PICOTTI, *Presentazione*, in ID. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet,* Padova, 2004, VII; PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, cit., 47 ss.

[118] Per approfondimenti sul punto v. FLOR, *Lotta alla "criminalità informatica"*, cit., 3 e 4.

[119] PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, cit., 75: tra le locuzioni presenti nei reati informatici "in senso stretto" si ravvisano, a titolo esemplificativo, le seguenti: «intervenire senza diritto su dati, informazioni o programmi informatici; introdursi o mantenersi in un sistema informatico o telematico; alterare od ostacolare il funzionamento di un sistema informatico o telematico; contraffare, alterare o sopprimere un documento informatico; prendere cognizione, sopprimere od alterare corrispondenza informatica o telematica, ecc.».

su oggetti tecnici, ovvero includere le tecnologie dell'informazione e della comunicazione, compreso il *web,* nella condotta tenuta o nel risultato che ne deriva. In tal caso, quindi, gli elementi tipizzanti della fattispecie compaiono nella sua formulazione legislativa solo come possibile modalità, oggetto o effetto della condotta, in sostituzione di equivalenti legali che ignorano le suddette tecnologie. Addirittura, talvolta, non vi è alcun riferimento espresso a tali elementi distintivi, i quali possono essere ricavati in via interpretativa dalla norma[120].

Rientrano dunque in questa categoria, flessibile e soggetta ad un continuo ampliamento[121], tutte quelle fattispecie "comuni" che, anche se non prevedono esplicitamente elementi caratteristici afferenti alla tecnologia, risultano comunque applicabili a situazioni poste in essere per mezzo delle TIC e della rete[122].

Anche nella più ampia categoria dei reati cibernetici, ossia di quei reati che si commettono, o possono essere realizzati, in rete o nel *cyberspace*, quale conseguenza e dimostrazione del suesposto passaggio cruciale dai *computer crimes* ai *cybercrimes*, è possibile distinguere i reati cibernetici in senso stretto dai reati cibernetici in senso ampio.

Si considerano reati cibernetici in senso stretto quei reati la cui formulazione legislativa include esplicitamente un elemento tipizzante che richiama espressamente la rete o il *cyberspace*. Diversamente, nei reati cibernetici in senso ampio gli elementi caratteristici del fatto di reato che si riferiscono alla rete o al *cyberspace* sono contemplati solo in modo implicito nella norma o ricavabili dalla sua interpretazione. Nei primi, la commissione del fatto in rete è un requisito esplicitamente e incontestabilmente indicato dal legislatore ai fini della configurabilità della fattispecie; nei secondi, invece, formulati in termini più generici e flessibili, il riferimento alla rete, o al *cyberspace*, è solo eventuale, quale possibile modalità, oggetto o conseguenza della condotta, e deducibile anche solo in via ermeneutica[123]; ad ogni modo si tratta di reati «realizzabili o concepibili a prescindere dall'informatica e dalla rete »[124].

---

[120] *Ivi*, 76.

[121] *Ivi*, 77.

[122] V. FLOR, *Lotta alla "criminalità informatica"*, cit., 3 e 4.

[123] *Ivi*, 5; PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, cit., 77 s.

[124] FLOR, *Lotta alla "criminalità informatica*", cit., 5.

I reati cibernetici "in senso stretto" sono anche reati informatici "in senso stretto", poiché l'elemento che richiama la commissione "in rete" o nel *cyberspace* comporta inevitabilmente un riferimento espresso alle tecnologie dell'informazione e della comunicazione. Al contrario, non tutti i reati informatici in "senso stretto" sono anche reati cibernetici "in senso stretto", poiché l'elemento che invoca le TIC, nei primi, non necessariamente esige anche la commissione in rete, propria dei secondi; infatti i reati informatici "in senso stretto" rientrano nella categoria dei reati cibernetici "in senso ampio", in ragione della sola eventualità che si realizzino nel cyberspazio[125].

I crimini informatici si differenziano tra loro, per modalità operative e finalità della condotta, in: crimini con scopo di profitto per l'autore e di danno per la vittima; crimini rivolti contro l'elaboratore al fine di distruggerlo o renderlo inutilizzabile; crimini associati all'uso del computer per nuocere ai singoli o all'intera collettività[126].

I reati informatici sono classificati nel codice penale rispettando il tradizionale criterio del bene giuridico offeso, ma nell'ambito della criminalità informatica accanto ai classici beni giudici tutelati si affiancherebbero "nuovi" interessi, inesistenti prima dell' avvento delle TIC e derivanti dalla continua evoluzione del *modus operandi* degli illeciti, tra i quali, secondo alcuni autori, si ravviserebbe il "bene giuridico informatico", riconducibile alla diffusione dei sistemi di trattamento, trasmissione, memorizzazione ed elaborazione di dati, il quale, infatti, necessita di protezione non solo tecnica ma anche giuridica[127]. Sembrerebbe possibile individuare tre categorie di reati informatici in base al diverso atteggiarsi dei beni giuridici tutelati e delle possibili modalità di offesa: il primo riferimento è diretto alle fattispecie poste a tutela di beni giuridici tradizionali, aggrediti da nuovi mezzi o con nuove modalità; in secondo luogo

[125] V. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, cit., 78.

[126] Sul punto CUOMO, RAZZANTE, *La disciplina dei reati informatici*, cit., 6.

[127] *Ivi*, 7; sul punto si esprime anche AMATO, DESTITO, DEZZANI, SANTORIELLO, *I reati informatici. Nuova disciplina e tecniche processuali di accertamento*, Padova, 2010, 11 ss., secondo cui le diverse figure criminose rientranti nella criminalità informatica non presenterebbero un medesimo bene giuridico, per cui unificare il diritto penale dell'informatica intorno ad un unico oggetto di tutela, da individuare nell' "affidabilità e sicurezza del ricorso alla tecnologia informatica, telematica e cibernetica", non sembrerebbe una tesi condivisibile, infatti i diversi reati informatici sono stati inseriti nel codice penale in titoli e capi preesistenti , in base al bene giuridico protetto.

emergono le offese a beni giuridici analoghi a quelli tradizionali, la cui condotta ricade su nuovi oggetti "passivi", e tale diversità si riflette sui beni tutelati; l'ultima tipologia riguarda tutte quelle figure di reato in cui i beni giuridici offesi appaiono come "nuovi", poiché manifestatasi con le TIC[128].

Tra i beni giuridici, vecchi e "nuovi", lesi dalla delinquenza informatica, a titolo esemplificativo, vi sono il patrimonio, la fede e l'ordine pubblico, il domicilio, l'integrità e la sicurezza informatica, la confidenzialità, la segretezza e la riservatezza dei dati personali in rete, sottolineando la presenza di molteplici ambiti d'interesse, tra cui il diritto d'autore[129].

Tuttavia, sembra opportuno precisare già da ora che il legislatore del '93 non ha inteso considerare le nuove forme criminose come aggressive di beni giuridici nuovi rispetto a quelli già tutelati dalle fattispecie incriminatrici esistenti[130].

Va inoltre specificato che gli interessi e i valori tradizionali devono essere egualmente tutelati, poiché soggetti ad innovativi e più aggressivi attacchi dovuti principalmente alle tipicità della rete.

La condotta dell'agente deve indirizzari ad un computer o perlomeno presupporre l'impiego di uno strumento tecnologico meccanizzato; le azioni degli utenti infatti ricadono sul sistema informatico, o sul sistema telematico, quali oggetti materiali d'interesse, costituenti la categoria che il legislatore intende proteggere, poiché relativa a sistemi, reti e infrastrutture di primaria importanza per la società attuale[131].

La legge del'93, introduttiva dei *computer crimes,* non aveva previsto alcuna definizione di "sistema informatico", e, per colmare tale lacuna, la giurisprudenza ne ha elaborata una, in linea di massima, adeguata a tutte le fattispecie che contemplano tale termine, assumendo una nozione quanto più

---

[128]In argomento PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in ID (a cura di), *Il diritto penale dell'informatica nell'epoca di internet*, Padova, 2004, 54 s. e 70: «Si può al riguardo parlare di beni giuridici "nuovi", in quanto non trovano precisa corrispondenza in altri preesistenti, benché una certa analogia sia sempre ravvisabile e la distinzione dalle ipotesi tradizionali non sia, per forza di cose, così netta come la partizione esposta potrebbe fari ritenere».

[129] CUOMO, RAZZANTE, *La disciplina dei reati informatici*, cit., 7 s.

[130] AMATO, DESTITO, DEZZANI, SANTORIELLO, *I reati informatici*, cit., 11 ss.

[131] CUOMO, RAZZANTE, *La disciplina dei reati informatici*, cit., 8.

generica e inclusiva al fine di scongiurare vuoti di tutela. In particolare, essa ritiene che la locuzione "sistema informatico" si rivolge a «il concetto di una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all' uomo, attraverso l'utilizzazione (anche in parte) di tecnologie informatiche»[132].

Il sistema informatico, quale oggetto materiale delle condotte incriminate, è costituito da due componenti tra loro complementari: una parte fisica, denominata *hardware* e composta da apparati ed elementi materiali; una parte logica, relativa alle procedure elettroniche e ai programmi di base, definita *software*[133]. L' elemento essenziale che consente di definire il sistema come "informatico" si individua nell'idoneità dell'*hardware* a programmare ed elaborare i dati in base al *software*, per conseguire finalità diversificate[134]. In altri termini, affinché possa parlarsi di sistema informatico è essenziale che vi sia l'elaborazione automatica di un elevato numero di dati in formato digitale attraverso elaboratori.

In base a quanto specificatamente disposto dall'art. 1 della Convenzione di Budapest, il sistema informatico corrisponde a «qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dei dati»[135].

Il sistema telematico, invece, si riferisce ad un insieme di apparecchi addetti alla trasmissione a distanza di informazioni e dati, per mezzo dell'utilizzo di tecnologie dedicate alle telecomunicazioni[136].

La tradizionale concezione di condotta concepita per la realtà fisica muta di significato nell'ambiente informatico e telematico, infatti le azioni penalmente rilevanti, nell'ambito della criminalità informatica, dipendono dall'interazione che avviene tra l'utente e il sistema, originando forme di trasmissione, immissione e gestione di dati che si sostanziano di impulsi elettronici che avviano il computer,

---

[132] *Ivi*, 9., che richiama Cass. pen., Sez.VI, 4 ottobre 1999, n. 3065, De Vecchis, in *Cass. pen*., 2001, 481.

[133] CUOMO, RAZZANTE, *La disciplina dei reati informatici*, cit., 12.

[134] *Ivi*, 10 s.

[135] V. *Convenzione di Budapest* 23 novembre 2001, art. 1.

[136] Cfr. CUOMO, RAZZANTE, *La disciplina dei reati informatici*, cit., 13: «Il collegamento tra più sistemi informatici deve soddisfare alcuni requisiti essenziali: a) la connessione deve avere carattere stabile (attraverso canali di comunicazione televisivi, satellitari, telefonici, via etere) o permanente (LAN o rete collegato via cavo); b) lo scambio di informazioni e la connessione tra elaboratori distanti deve essere il mezzo necessario per conseguire le finalità operative del sistema».

inducendolo ad eseguire una serie di operazioni con chiare finalità illecite, i cui effetti sono, talvolta, rilevabili anche nella realtà fisica.

A differenza dei reati tradizionali in cui gli effetti della condotta sono rilevabili nel luogo in cui i trova l'agente, le conseguenze dannose della condotta rivolta a dispositivi tecnologici automatizzati, e posta in essere sfruttando il collegamento tra sistemi topograficamente distanti, possono prodursi, anche simultaneamente, in tempi e in luoghi diversi da quelli in cui la condotta è stata commessa, causando non pochi problemi nella ricerca del colpevole[137].

Inoltre, tra i soggetti attivi emerge un elevato senso di sicurezza, derivante principalmente dal presunto anonimato garantito dalla rete, il quale contribuisce a fomentare la commissione di condotte illecite, falsando e riducendo la percezione del rischio di essere individuati e puniti, nonché rafforzando così la comune sensazione di impunità [138]. I criminali risultano desensibilizzati, poiché avvertono come meno gravi le condotte realizzate nel *cyberspace*, non solo in virtù della lontananza fisica rispetto alla vittima, ma anche perché sono soliti considerare tale dimensione sprovvista di regole e confini. Si registra dunque la proliferazione non solo dei reati tradizionali commessi in rete, ma anche degli illeciti perpetrabili unicamente attraverso lo strumento informatico.

I reati informatici sono considerati reati comuni, potendo essere commessi da chiunque, sebbene spesso possano essere realizzati da una particolare categoria di soggetti, qualificati come "operatori di sistema". Si tratta di una qualità che può essere assunta da un'ampia gamma di soggetti, tra cui quelli che svolgono operazioni di *input* e di *output*, di attivazione e di interruzione del computer, i programmatori che indicano istruzioni e operazioni all'elaboratore che è tenuto ad effettuarle, i sistemisti che studiano i sistemi al fine di massimizzarli e gli analisti che elaborano algoritmi per ottemperare a specifiche esigenze[139]. In linea generale è stato osservato che «l'operatore del sistema non è soltanto colui che professionalmente, in via continuativa quantomeno non occasionale, si trova ad

[137] *Ivi*, 14 s.

[138] In argomento BALLONI, BISI, SETTE, *Principi di criminologia applicata.* cit., 271 e s.

[139] V. CUOMO, RAZZANTE, *La disciplina dei reati informatici*, cit., 23 s., ove si precisa che «l'esercizio delle mansioni deve comportare la conoscenza del funzionamento del sistema e deve tradursi in attività di manutenzione, attivazione o controllo a prescindere dall' esistenza di un rapporto di lavoro con il titolare dell'elaboratore elettronico».

interagire sull' *hardware* o sul *software* di un sistema informatico, ma anche il soggetto che, di fatto si trova nella condizione di poter intervenire, direttamente o per interposta persona, a causa delle sue funzioni, sui dati o sui programmi»[140], infatti non è richiesta alcuna relazione di proprietà con il sistema. Sembra essere inoltre una qualifica attribuibile sia a persone fisiche che a persone giuridiche.

Le azioni illecite poste in essere da chi ricopre il suddetto ruolo e abusa della propria qualifica costituiscono ipotesi aggravate, appositamente previste da alcune fattispecie di reato.

La previsione di questa aggravante speciale ed il conseguente inasprimento del trattamento sanzionatorio sono giustificati dal maggiore disvalore attribuito alla condotta dei soggetti attivi, ai quali si riconosce una posizione di vantaggio, in ragione della sussistenza del particolare rapporto fiduciario tra gli stessi e il bene giuridicamente tutelato; gli agenti, in ragione della qualità suindicata, possono accedere ad aree riservate e controllare le operazioni ivi compiute, risultando agevolati nella commissione del crimine, poiché dinanzi alle loro condotte offensive le misure protettive previste risultano inefficienti.

Sembra altresì opportuno evidenziare che ai fini dell'integrazione della suddetta circostanza aggravante speciale rileva non solo l'abusività della condotta, ma anche lo svolgimento di un'attività diversa da quella autorizzata[141].

Si intende infine precisare, senza entrare nei dettagli, che ulteriore soggetto qualificato che può assumere la titolarità dei reati informatici è il *provider*, il quale gestisce la rete su cui circolano i dati, consentendo agli utenti, gratuitamente o a pagamento, l'accesso ad internet; si tratta di una figura intermedia tra colui che inserisce i dati e gli utenti finali, poiché le trasmissioni digitali all'interno delle reti telematiche non sono dirette, ma le informazioni, prima di divenire accessibili al pubblico, si imbattono in dette figure interposte. Anche in tal caso, in virtù del

[140] *Ivi*, 25.

[141] *Ibidem*: «Il fondamento dell'aggravante va ricercato nella "speciale opportunità" del soggetto attivo di sfruttare le proprie conoscenze per la commissione del reato a causa dell'esistenza di un rapporto giuridico di qualsivoglia natura, a carattere anche saltuario o temporaneo, con il bene su cui ricade la condotta materiale».

particolare ruolo svolto, l'eventuale responsabilità imputabile al *provider* risulterà aggravata[142].

Esaurita l'analisi delle caratteristiche essenziali dei reati informatici e cibernetici, è bene concentrarsi ora sul quadro normativo di riferimento.

1.3 Le fonti sovranazionali e l'evoluzione della normativa italiana per il contrasto alla criminalità informatica

Come preannunciato, si deve all'incessante sviluppo tecnologico e alla determinante imposizione della dimensione cibernetica l'origine e l'evoluzione di nuove forme di aggressione, sempre più sofisticate e complesse, e del conseguente e più ampio fenomeno della delinquenza informatica e cibernetica, volti a pregiudicare un numero sempre crescente di diritti e di interessi esigenti di adeguata tutela. Si è progressivamente manifestata la necessità di creare sistemi armonici d'incriminazioni e sanzioni penali, fondati sulla collaborazione nazionale e sovranazionale, pubblica e privata. Proprio per rispondere a tale necessità, ed ovviare alle perseveranti minacce, negli anni è stato predisposto un articolato *framework* normativo, quale risultato di innumerevoli interventi legislativi nazionali e sovranazionali, intesi a contrastare il complesso scenario della criminalità informatica e più in generale cibernetica, poiché la rete non può essere considerato un luogo esente dal diritto.

Emerge un'inedita riconsiderazione di concetti ordinari, come quelli di spazio e azione penalmente rilevante, finalizzata a reprimere le innovative condotte criminose, sottolineando talvolta l'inadeguatezza delle classiche figure di reato e delle tradizionali norme penali.

Il quadro normativo in esame è da intendersi in costante evoluzione, in concomitanza con lo sviluppo tecnologico, poiché la realtà giuridica deve sempre adeguarsi alla realtà digitale e prevenire, laddove possibile, qualunque tipo di minaccia.

Le prime indicazioni giuridiche relative a tale inedito contesto sono comparse in Italia intorno alla fine degli anni '70, quando il legislatore è stato

[142] CUOMO, RAZZANTE, *La disciplina dei reati informatici*, cit., 25 ss.; AMATO, DESTITO, DEZZANI, SANTORIELLO, *I reati informatici*, cit., 17 s.

obbligato ad intervenire per fronteggiare nuovi eventi lesivi dei beni giuridici tutelati dall'ordinamento, in ragione dell'insuperabilità dei rigorosi limiti sanciti dai principi di tassatività e tipicità. Tra i primi interventi settoriali, sporadici e frammentari, riguardanti rilevanti fatti cronaca, vi sono quelli riguardanti l'attentato e il sabotaggio ad impianti e centri di elaborazione di dati, e quelli relativi alle iniziali forme di "frodi" avverso i sistemi informatici di gestione contabile delle imprese assicurative e bancarie[143] .

Negli stessi anni, in molti casi, dinnanzi al silenzio del legislatore, dottrina e giurisprudenza si sono adoperate per ricondurre le nuove condotte criminose a fattispecie esistenti, operazione rivelatasi particolarmente agevole nel caso in cui fosse stato l'*hardware*, ossia la componente materiale del sistema informatico, l'oggetto materiale della condotta incriminata, facendo rientrare il fatto nelle ipotesi tradizionali di danneggiamento o furto; al contrario, questa si mostrava nettamente più complessa nel caso in cui il comportamento fosse ricaduto sulla parte logica del sistema, vale a dire il *software*. Questo è il caso, ad esempio, della frode perpetrata per mezzo dell'elaboratore, tipica ipotesi di impiego fraudolento di un sistema informatico, rispetto al quale si è posto un annoso dibattito sulla possibile configurabilità del delitto di truffa *ex* art. 640 c.p.

Al riguardo, la dottrina maggioritaria tendeva ad escludere la suindicata possibilità, poiché l'alterazione del funzionamento del sistema informatico induceva in errore il sistema stesso e non la persona fisica – dato testuale che non poteva essere forzato in virtù del divieto di analogia in *malam partem.* Si faceva dunque sempre più pressante l'esigenza di un'adeguata e specifica tutela che fosse capace di trovare una soluzione sanzionatoria appropriata per le nuove condotte criminose, consistenti nell'utilizzo illecito degli strumenti informatici e telematici.

Nel contempo, si sviluppava un dibattito giuridico sui *cybercrimes*, in ragione non solo dei dilemmi sostanziali e processuali tipici del nuovo ambiente, ma anche del suddetto bisogno di protezione manifestato dagli utenti, i quali rivendicavano il loro diritto alla sicurezza e al libero utilizzo degli strumenti informatici. Le stesse perplessità venivano sollevate contestualmente anche a

[143] In argomento PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, cit., 26; FARINA, *Elementi di diritto dell'informatica*, Padova, 2019, 242.

livello europeo, in virtù della piena consapevolezza che per un completo sviluppo sociale non si potesse prescindere dalla previsione di un quadro normativo armonico nei diversi Paesi, che fosse idoneo a regolare il fenomeno[144].

Sul piano internazionale, nel 1983, l'OCSE ha svolto uno studio sul possibile allineamento delle leggi penali, proprio al fine di contrastare la delinquenza informatica, pubblicando inoltre, nel 1986, una relazione denominata "*Computer-Related Crime: Analysis of Legal Policy*" in cui ha analizzato le normative in vigore ed ha proposto potenziali riforme, formulate da alcuni Stati membri, suggerendo strumenti penali da adottare per la lotta al crimine informatico. Nel 1992, la stessa organizzazione per la cooperazione e lo sviluppo economico ha sollecitato gli Stati ad assumere mezzi di difesa per la protezione dei sistemi informatici[145].

Nel 1989 è stata adottata dal Comitato dei ministri del Consiglio d'Europa la Raccomandazione sulla criminalità informatica n. (89)9, quale pilastro di riferimento internazionale che ha individuato due diverse liste, una minima e una facoltativa, a cui ricondurre le condotte criminose sulla base della necessità di repressione obbligatoria, nel primo caso, o discrezionale, nel secondo. La ragione basilare propria della scelta di due liste è da attribuire alla mancanza di una visione univoca sul metodo di contrasto alla criminalità informatica, benché si incoraggi il ricorso a mezzi di natura penale, invitando gli stati ad intervenire uniformemente.

Nella lista minima sono ricompresi i più gravi comportamenti, i quali devono pertanto essere obbligatoriamente incriminati, esortando talvolta gli Stati a prevedere interventi legislativi appositi. Tra le condotte più gravi compaiono la frode informatica, il sabotaggio informatico, il falso in documenti informatici e l'accesso non autorizzato al sistema informatico o alla rete telematica[146].

La lista facoltativa, al contrario, si riferisce all'insieme di condotte che solo eventualmente sono punibili in sede penale, poiché è lasciata alla discrezionalità e all'autonomia degli Stati la scelta sul tipo di intervento da porre in essere, adottando, se opportuno, anche strumenti sanzionatori alternativi. Rientrano, tra gli

---

[144] *Ivi*, 242.

[145] V. FLOR, Cyber-criminality*: le fonti internazionali ed europee*, in CADOPPI, CANESTRARI, MANNA, PAPA (diretto da), Cybercrime, Torino, 2019, 99.

[146] Per uno sguardo alla lista minima v. FARINA, *Elementi*, cit., 243.

altri, in tale lista l'alterazione di dati o programmi informatici non consentita e lo spionaggio informatico [147].

Ulteriore rilevante Raccomandazione del Consiglio d'Europa, è quella approvata l'11.9.1995, n. (13)95, riferita al settore procedurale. Tale Raccomandazione si propone di fornire una risposta ai crimini informatici, sottolineando il rischio proprio dell'utilizzo di sistemi informatici per commettere reati, rinviando alla Raccomandazione n. (9)89, e manifestando l'esigenza di assicurare mezzi e garanzie adeguati nella ricerca e nella raccolta delle c.d. "prove elettroniche".

Altro oggetto della Raccomandazione si ravvisa nell'opportunità di introdurre l'obbligo per i *service providers* di fornire le opportune misure per consentire l'intercettazione delle telecomunicazioni, consentendo alle Autorità investigative di individuare i soggetti coinvolti[148].

Nel 1997 viene poi istituito, all'interno del consiglio d' Europa, il Comitato di Esperti sulla Criminalità nel *Ciberspazio* incaricato di predisporre una Convenzione internazionale per il contrasto alla criminalità informatica, tenendo conto di tutte le peculiarità proprie del nuovo mondo, al fine di favorire la cooperazione internazionale e facilitare le attività di investigazione e rilevamento dei *computer crimes*. Dopo quattro anni di lavoro è stata adottata, il 23 novembre del 2001, la Convenzione sulla criminalità informatica, più comunemente conosciuta come Convenzione di Budapest[149].

Il Consiglio dell'Unione Europea, il 24 febbraio del 2005, ha varato la Decisione Quadro 2005/222/GAI, concernente gli attacchi contro i sistemi di informazione, con l'intento di fortificare la collaborazione tra le Autorità giudiziarie e le altre Autorità competenti degli Stati membri, per mezzo del ravvicinamento e dell'armonizzazione delle legislazioni penali nel campo degli attacchi avverso i sistemi di informazione. Si tratta di una Decisione che rendeva obbligatoria la criminalizzazione di condotte strettamente definite, e diversamente dalla

[147] Per uno sguardo alla lista facoltativa v. FARINA, *Elementi*, cit., 243.

[148] FLOR, Cyber-criminality*: le fonti internazionali ed europee*, cit., 100 ss.

[149] SARZANA DI S. IPPOLITO, *Informatica, Internet e diritto penale,* cit., 587 ss.; FLOR, *Cyber-criminality: le fonti internazionali ed europee*, cit., 101.

convenzione di Budapest, non riguardava tutti i reati, ma solo gli attacchi informatici, applicandosi solo agli Stati membri[150].

La suddetta Decisione quadro è stata sostituita dalla Direttiva 2013/40/UE del Parlamento Europeo e del Consiglio, con il medesimo obiettivo «di ravvicinare il diritto penale degli Stati membri nel settore degli attacchi contro i sistemi di informazione, stabilendo norme minime relative alla definizione dei reati e delle sanzioni rilevanti, e migliorare la cooperazione fra le autorità competenti, compresi la polizia e gli altri servizi specializzati degli Stati membri incaricati dell'applicazione della legge, nonché le competenti agenzie e gli organismi specializzati dell'Unione, come *Eurojust, Europol* e il suo Centro Europeo per la criminalità informatica, e l'Agenzia Europea per la sicurezza delle reti e dell'informazione (ENISA)»[151]. Essa si fonda sull'assunto che il corretto funzionamento e la sicurezza dei sistemi informatici siano funzionali allo sviluppo del mercato interno e di un'economia concorrenziale.

Nella Direttiva 2013/40/UE si ravvisano lievi differenze rispetto alla sostituita Decisione quadro, tra le quali «l'obbligo per gli Stati di incriminare la condotta di intercettazione illecita di comunicazioni informatiche o telematiche, e la previsione della reclusione non inferiore nel massimo a due anni per le condotte di fabbricazione, vendita, approvvigionamento per l'uso, importazione e distribuzione o messa a disposizione in altro modo di software destinati o modificati principalmente al fine di commettere uno dei reati previsti dalla direttiva nonché di password e codici d'accesso che permettono di accedere in tutto o in parte a un sistema di informazione per la commissione degli stessi reati»[152].

1.3.1 La legge n. 547/1993

Le indicazioni previste dalla Raccomandazione n. (89)9 sono state recepite dal legislatore italiano con la Legge 23 Dicembre 1993, n. 547, relativa alle "Modificazioni ed integrazioni alle norme del codice penale e del codice di

[150] Sul punto SARZANA DI S. IPPOLITO, *Informatica, Internet e diritto penale,* cit., 627 ss.
[151] Cfr. Considerando 2 della Direttiva 2013/40/UE.
[152] V. CONIGLIARO, *La nuova tutela penale europea dei sistemi di informazione. Una prima lettura della direttiva 2013/40/UE del Parlamento europeo e del Consiglio*, in *Dir. pen. cont.*, 30 ottobre 2013, 2.

procedura penale in tema di criminalità informatica", la quale ha determinato un cambiamento rivoluzionario nell'ordinamento giuridico italiano[153]. Si tratta di una riforma predisposta in un contesto nazionale costantemente esposto a rischi derivanti dell'utilizzo degli strumenti informatici e telematici, e che ha pertanto introdotto nuove fattispecie di reato, incidendo anche sulle condotte già codificate. In generale, la suddetta riforma ha regolato tutte quelle condotte illecite che integravano, ed integrano tutt' oggi, i reati informatici.

Come preannunciato, prima del '93 vi erano stati pochi e settoriali interventi legislativi, frammentari e sporadici, e alcuni tentativi da parte di dottrina e giurisprudenza di ricondurre i nuovi comportamenti alle fattispecie esistenti.

La Legge n. 547/93, c.d. "Legge Conso", ha rappresentato la prima risposta concreta, a livello nazionale, alla più volte citata esigenza di adeguata tutela contro le nuove forme di aggressione informatica, avendo introdotto nell'ordinamento penale italiano i *computer crimes*; ad essa, inoltre, si riconosce il grande merito di aver posto fine alle continue trasgressioni del principio di tassatività, consentendo altresì l'allineamento della legislazione interna alle disposizioni sovranazionali.

Ad ogni modo, nell'ambito della Legge Conso, per il legislatore è stato piuttosto complesso effettuare la scelta delle condotte da incriminare in base all'interesse da tutelare, infatti a tal proposito non sono mancate critiche relative alla formulazione di alcune fattispecie, o per non aver tenuto conto dei possibili effetti attribuibili a ciascuna di esse.

Da un lato, i nuovi mezzi di repressione penale in ambito tecnologico sono inseriti nel codice a titolo di aggiornamento di norme già esistenti, includendovi, dunque, le nuove modalità di aggressione del bene giuridico; dall'altro lato, si ravvisa l'introduzione di ulteriori ed innovative figure criminose, ovverosia i c.d. *computer crimes*, benché molto simili a quelle vigenti a cui si sarebbe fatto ricorso se la condotta fosse stata attuata senza il tramite degli strumenti informatici[154].

---

[153] Cfr. PICOTTI, *Sistematica dei reati informatici*, cit., 28: «[…]un vero e proprio punto di svolta nell'evoluzione del diritto penale dell'informatica, perché ha "chiuso" la fase schematicamente definibile del computer-crime "classico", e dopo di essa si è aperta quella attuale, definibile del *cybercrime*».

[154] Sul punto FARINA, *Elementi di diritto dell'informatica,* cit., 245.

Va precisato altresì che la scelta sistematica compiuta del legislatore relativamente alla previsione dei crimini informatici si basa sull'individuazione dei beni giuridici da tutelare, benché nel corso dell'*iter* legislativo[155] si fosse affacciata l'ipotesi di prevedere un apposito titolo da riservare esclusivamente ai delitti in materia informatica e telematica, o addirittura, in alternativa alla modifica del Codice, di introdurre una legge penale speciale[156].

La scelta effettuata dalla Commissione Ministeriale di inserire le nuove figure criminose in corrispondenza delle fattispecie già previste, e protettive dei medesimi beni giuridici, nonché di aggiornare le stesse, laddove possibile, con i riferimenti tecnologici, si basa principalmente sul fatto che si tratta di nuove forme di violenza, le quali si distanziano dalle figure criminose tradizionali per il mezzo utilizzato o per l' oggetto materiale su cui ricade la condotta, riferendosi però a beni giuridici già tutelati in altre parti del codice; sarebbe pertanto risultata inadeguata la decisione di prevedere un apposito titolo nel codice penale, o addirittura promuovere una legge speciale *ad hoc*[157].

Sembra opportuno puntualizzare, quindi, che non si può prescindere dall'individuazione dei beni giuridici tutelati, poiché è in base ad essi che si può incriminare una condotta o ricostruire la natura e la categoria dei reati, conformemente al principio di offensività, per cui il legislatore è obbligato a delineare i crimini come forme di offesa ai beni giuridici[158]; «il nostro sistema

---

[155] V. SARZANA DI S. IPPOLITO, *Informatica, Internet e diritto penale,* cit.,183 ss.

[156] *Ivi*, 187.

[157] Cfr. SARZANA DI S. IPPOLITO, *Informatica, Internet e diritto penale,* cit., 187; v. altresì FARINA, *Elementi*, cit., 245 ss.: «Altre autorevoli Voci, però, hanno rinvenuto nelle nuove fattispecie di criminalità informatica l'emersione di un nuovo bene giuridico, da qualcuno inquadrato come "l'intangibilità informatica", da intendersi come "l'esigenza di non alterare la relazione triadica fra dato e realtà, rispettiva informazione e soggetti legittimati ad elaborare quest'ultima nelle sue diverse fasi (creazione, trasferimento, ricezione)"; da altri, individuato "nell'esclusiva disponibilità della tecnologia informatica" per il soggetto legittimato; infine, da qualcun altro, come bene informatico, ossia "oggetto di un nuovo diritto di carattere reale, ossia di inerenza del diritto al bene che ne rappresenta l'oggetto, di *jus in re* propria, anche se si tratta di una res o cosa immateriale, come lo sono del resto anche i prodotti intellettuali, ma che è stata resa oggettiva, cioè misurabile in termine di valore economico" (...)Va, infine, ricordata, più che altro per ragioni di completezza, la Voce di chi, constatando la sempre più ampia diffusione di Internet, ha sostenuto che la sussistenza di un "nuovo diritto soggettivo di libertà personale, precedentemente sconosciuto: il diritto di libertà informatica", da considerare il comune denominatore delle nuove fattispecie incriminatrici.(…)».

[158] V. FARINA, *Elementi,* cit., 245, che richiama in nota, sull'argomento, MARINUCCI, DOLCINI, *Costituzione e politica dei beni giuridici*, in *Riv. it. dir. proc. pen*., 1994, 2, 333-373 e BERGHELLA, BLAIOTTA, *Diritto penale dell'informatica e beni giuridici*, in *Cass. pen.*, 1995, 9, 2329-2343; si sottolinea, altresì, che il sistema penale italiano si fonda sul ricorso al reato, inteso

penale, infatti, è ispirato al modello garantistico liberale del diritto penale del fatto» [159].

Senza voler entrare nel merito delle singole novità previste, ci limitiamo qui ad accennare che la Legge n. 547/1993 è intervenuta in quattro diversi settori, ossia quattro macro-categorie.

Il primo ambito d'intervento è quello delle frodi informatiche, poste in essere per mezzo di strumenti tecnologici, che si caratterizza per l'introduzione dell'art. 640-*ter* nel codice penale. Una simile operazione è dovuta alla commissione di condotte non reprimibili alla stregua del delitto di truffa comune, tema su cui si avrà modo di approfondire in seguito.

La seconda area interessata concerne la falsificazione di documenti informatici, tipica forma di abuso della tecnologia; mentre il terzo settore su cui si interviene riguarda l'integrità dei dati e dei sistemi informatici; e, infine, l'ultimo ambito è quello della riservatezza dei dati e delle comunicazioni informatiche[160].

Tra le principali novità inserite nel codice penale dalla Legge Conso è meritevole di menzione l'art. 615-*ter* c.p., relativo all' accesso abusivo ad un sistema informatico o telematico, formulato sulla falsariga del tradizionale reato di violazione di domicilio, di cui all'art. 614 c.p. Esso è volto pertanto a proteggere tutti i sistemi dotati di misure di sicurezza da indebite intrusioni, vale a dire contro la volontà del titolare dello *ius excludendi*, sicché la *ratio* della presente norma è da ravvirarsi nell'esigenza di difesa della riservatezza[161].

Al di là delle innovazioni e delle modifiche apportate alla parte penale sostanziale, il legislatore è altresì intervenuto sulle norme processuali in materia di intercettazioni, ampliando così i mezzi di ricerca della prova[162].

Dopo aver proposto l'esame della Legge Conso, alla quale – come si è detto – si deve l'ingresso dei reati informatici nell'ordinamento penale italiano, sembra

---

come offesa al bene tutelato, e meritevole di un'adeguata sanzione penale, quale *extrema ratio*, nel rispetto del principio di sussidiarietà.

[159] Cfr. FARINA, *Elementi di diritto dell'informatica*, cit., 245.

[160] V. FOGLIANI, *I reati commessi su internet:* computer crimes *e* cybercrimes, in *www.fog.it*, 3 marzo 2009*;* NERI, *Criminologia e reati informatici. Profili di diritto penale dell'economia*, Napoli, 2014, 40.

[161] In argomento ANTOLISEI, *Manuale di diritto penale. Parte speciale*, Vol. I, Milano, 2016, 290 ss.

[162] Sul punto SARZANA DI S. IPPOLITO, *Informatica, Internet e diritto penale*, cit., 203 ss.

opportuno proseguire con l'analisi dei provvedimenti elaborati nel contesto sovranazionale.

1.3.2 La Convenzione di Budapest e la legge di ratifica n. 48/2008

Lo sviluppo tecnologico e l'avvento di Internet in particolare hanno favorito il processo di globalizzazione sociale ed economico, nonché la conseguente formazione di un contesto colmo di opportunità e rischi, in cui compaiono, come già detto, nuove forme di aggressione a beni giuridici tradizionali e innovativi. Nasce così un nuovo fenomeno, formato da condotte criminali a carattere transfrontaliero, che necessitano di norme omogenee globalmente valide, al fine di eludere condizioni di incertezza che favoriscono la proliferazione di situazioni di pericolo.

È in questa prospettiva che si realizza un grandioso progetto legislativo in materia di delinquenza informatica e cibernetica: la Convenzione del Consiglio d'Europa sul *cybercrime*[163]. Essa rappresenta, assieme alle Raccomandazioni del Consiglio d'Europa, lo strumento internazionale più importante nel contrasto al *cybercrime*, nonché un esempio di cooperazione internazionale e modello per tutti coloro che intendono legiferare in materia.

Tale Convezione è stata firmata a Budapest il 23 Settembre del 2001, in occasione della Conferenza sul *Cybercrime*, al termine dei lavori avviati dal Comitato di Esperti appositamente istituito nel 1997[164]. La suddetta Convenzione è entrata in vigore il 1° Luglio del 2004 , ricevute le cinque ratifiche, di cui almeno tre da parte degli stati membri del Consiglio, in osservanza dell'art. 36 della stessa, e ad oggi risulta sottoscritta da sessantacinque Paesi[165], tra i quali vi sono anche stati Extraeuropei che hanno partecipato alla sua elaborazione; essa è stata successivamente integrata dal Protocollo del 28 marzo 2003, riguardante azioni razziste e xenofobe perpetrate attraverso i sistemi informatici.

---

[163] MORALES GARCÌA, *La politica criminale nel contesto tecnologico. Una prima approssimazione alla Convenzione del Consiglio d' Europa sul* Cyber-Crime, in PICOTTI (a cura di), *Il diritto penale dell'informatica nell' epoca di internet*, Padova, 2004, 123 ss.

[164] V. SARZANA DI S. IPPOLITO, *Informatica, Internet e diritto penale,* cit., 587 ss.

[165] In argomento *Stato delle firme e ratifiche di trattato, Convenzione sulla criminalità informatica*, in www.coe.int, 2020.

La Convenzione non include precetti penali, ma "Raccomandazioni" agli Stati affinché inseriscano le norme penali nel proprio ordinamento[166]. In sostanza, in essa sono contemplati i principi fondamentali che devono indirizzare il legislatore nazionale nell'elaborazione delle norme penali[167], al fine di disciplinare uniformemente il settore in questione; inoltre dal testo emerge una valutazione politico-criminale circa l'uso delle TIC.

La Convenzione si compone di 48 articoli, suddivisi in quattro capitoli, e prevede norme di diritto penale sia sostanziale che processuale, trovando applicazione per tutti i delitti perpetrati mediante un sistema informatico o telematico, oltreché per qualunque altro crimine la cui raccolta delle prove debba avvenire in forma elettronica. In altre parole, la stessa ha lo scopo di armonizzare il diritto penale sostanziale e processuale degli Stati interessati, di dotare il diritto penale processuale nazionale dei poteri necessari per perseguire i crimini posti in essere mediante strumenti informatici e telematici, nonché favorire e rafforzare la creazione di un regime di cooperazione internazionale, facilitando lo scambio di informazioni.

Tra i suoi propositi si ravvisa quello di perseguire una politica criminale comune, incentivando la collaborazione tra gli Stati e tra gli organismi pubblici e gli enti privati, al fine di prevenire e accertare i delitti in materia, considerando tutti i mutamenti dovuti alla digitalizzazione e alla globalizzazione.

I quattro capitoli, infatti sono rispettivamente dedicati alle definizioni terminologiche, alle misure da adottare in relazione sia al diritto sostanziale che al diritto processuale nazionale, alla collaborazione internazionale e alle clausole finali[168].

Per quel che riguarda il diritto penale sostanziale, tutte le disposizioni, ad esclusione di quelle in materia di diritto d'autore, esigono che i reati siano commessi senza diritto, sul piano oggettivo, e intenzionalmente, sul piano soggettivo[169]; in

---

[166] V. MORALES GARCÌA, *La politica criminale nel contesto tecnologico*, cit., 137.

[167] Ivi, 124: «[…]essa non contiene, dunque, un mandato a dare letterale trasposizione alla singola norma giuridica, bensì il mandato[…] a trasporre i suoi principi».

[168] In argomento SARZANA DI S. IPPOLITO, *Informatica, Internet e diritto penale,* cit., 589.

[169] Cfr. FLOR, Cyber-criminality*: le fonti internazionali ed europee*, cit., 102: «I reati informatici sono ripartiti in quattro "titoli", dedicati rispettivamente ai reati "contro la riservatezza, l'integrità e la disponibilità dei dati e sistemi informatici" (art. 2: accesso abusivo a sistemi informatici – art. 3: intercettazione abusiva – art. 4: attentato all'integrità dei dati – art. 5: attentato

alcuni casi, come accade per la frode informatica, è necessario altresì il dolo specifico[170].

Sul piano processuale e dei mezzi di ricerca della prova, la Convenzione suggerisce agli Stati di adottare una serie di disposizioni funzionali alla ricerca, raccolta e conservazione dei dati informatici, specie se vulnerabili[171].

Risulta inoltre rilevante la parte dedicata alla cooperazione internazionale, con riferimento alla reciproca assistenza per le indagini o per i procedimenti relativi a reati informatici, nonché per la raccolta di prove in formato elettronico, ed istituisce, a tal proposito, anche dei *contact points* al fine di garantire un sostegno immediato[172].

In conclusione, la Convenzione prospetta una serie di regole minime e di garanzie funzionali ad assicurare la protezione dei beni minacciati da un fenomeno che, nel tempo, ha assunto sempre più una natura transnazionale, e che necessita di uniformità legislativa e di una risposta coordinata a livello internazionale.

Sul piano dell'ordinamento interno, il legislatore italiano ha recepito la Convenzione di Budapest con ampio ritardo, ratificandola con la Legge 18 Marzo 2008, n. 48; essa ha rappresentato un significativo passo in avanti nella lotta contro il crimine informatico.

Tale legge è il risultato di un *iter* complesso che ha avuto inizio nel 2003, con l'istituzione di una Commissione interministeriale con il compito di redigere un disegno di legge di ratifica della Convenzione, ed è proseguito nel 2007, riprendendo in parte quanto precedentemente designato, concludendosi con l'approvazione del testo definitivo nel 2008[173]. Tuttavia, non sono mancate le critiche di chi ha definito la Legge di ratifica n. 48/2008 " frettolosa" – nonostante l'esteso lasso temporale impiegato per la sua elaborazione – poiché la stessa si sostanzia in un mero aggiornamento delle fattispecie esistenti, concernente

all'integrità del sistema – art. 6: abuso di dispositivi), alle "computer-related offences" (artt. 7: falsificazione informatica – art. 8: frode informatica), alle "content-related offences" (art. 9: pedopornografia) ed ai reati relativi alle violazioni del diritto d'autore (art. 10), nonché alla punibilità del tentativo e della complicità (art. 11). Il successivo art. 12 prevede l'inclusione dei reati informatici di cui alla CoC fra quelli per cui è prevista la responsabilità delle persone giuridiche».

[170] Cfr. SARZANA DI S. IPPOLITO, *Informatica, Internet e diritto penale,* cit., 591.

[171] In argomento *Ivi*, 600 ss.; FLOR, Cyber-criminality*: le fonti internazionali ed europee*, cit., 102 ss.

[172] V. FLOR, Cyber-criminality*: le fonti internazionali ed europee*, cit., 103 ss.

[173] V. SARZANA DI S. IPPOLITO, *Informatica, Internet e diritto penale,* cit., 632 ss.

interventi mirati e specifici su singole disposizioni, volto al miglioramento o all'adattamento delle stesse; dunque l' ambizioso piano di dare piena attuazione alla Convenzione sembra solo parzialmente realizzato, essendosi persa l'occasione di regolare complessivamente ed esaustivamente la materia relativa alla delinquenza informatica[174].

Una parte della dottrina ha infatti sottolineato con riguardo al diritto penale sostanziale che «il legislatore ha riformulato soltanto i reati di danneggiamento informatico: dal delitto-ostacolo concernente i "dispositivi" maligni (art. 615-*quinquies* c.p.), alle ben quattro ipotesi incriminatrici distinte a seconda che riguardino dati "privati" (art. 635-*bis* c.p.) o di "pubblica utilità" (art. 635-*ter* c.p.), sistemi informatici "privati" (art. 635-*quater* c.p.) o di "pubblica utilità" (art. 635-*quinquies* c.p.). La novella estende infine a tutti i reati informatici la responsabilità "amministrativa" delle persone giuridiche (*ex* d.lgs. 231/2001). Ma il complesso che ne risulta presenta incongruenze tecniche e sistematiche»[175]. Inoltre, tra gli interventi posti in essere, corrispondenti ad esigenze di riforma del diritto interno, non sono mancati «la soppressione della definizione di "documento informatico" ai fini penali (art. 491-*bis* c.p.), e l'introduzione di due nuovi delitti in materia di firme elettroniche (artt. 495-*bis* e 640-*quinquies* c.p.)»[176].

Per quanto riguarda i profili procedurali, le innovazioni previste dalla Legge di ratifica n. 48/2008 hanno riguardato principalmente i mezzi di ricerca della prova e le indagini di polizia giudiziaria. Tali interventi hanno assunto un rilievo tale da indurre l'interprete ad ampliare la portata teorica della novella al di là del settore proprio dei *cybercrimes*[177].

La normativa in esame ha adeguato l'ordinamento interno ad una delle più importanti fonti sovranazionali, con l'obiettivo di armonizzare i sistemi giuridici dei Paesi membri della Convenzione, proponendo un modello omogeno per il

---

[174] Sul punto FLOR, Cyber-criminality*: le fonti internazionali ed europee*, cit., 104.

[175] In argomento PICOTTI, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa, Profili di diritto penale sostanziale*, in *Dir. pen. proc.*, 2008, 6, 700 ss.

[176] V. FLOR, Cyber-criminality*: le fonti internazionali ed europee*, cit., 104.

[177] Per approfondire v. LUPÁRIA, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa. I Profili processuali*, in *Dir. pen. proc.*, 2008, 6, 717 ss.; cfr. FLOR, Cyber-criminality*: le fonti internazionali ed europee*, cit., 105: «non mancano comunque diversi profili critici in un assetto normativo ancora in larga parte perfettibile, soprattutto perché il tentativo di adattamento alle nuove sfide della società tecnologica è avvenuto principalmente seguendo uno stretto parallelismo con i tradizionali" mezzi di ricerca della prova, estesi a "dati, informazioni e programmi».

contrasto al crimine digitale e rafforzando il legame tra i profili sostanziali e quelli processuali. Da quanto si evince, tale intervento parziale e frammentario, seppur rappresentando l'idea di progresso, avrebbe potuto essere probabilmente maggiormente accurato e approfondito[178].

1.3.3 La Direttiva NIS e il d.lgs n. 65/2018

Si è più volte sottolineato che fine di garantire la sicurezza cibernetica è richiesto il rispetto delle regole da parte di tutti i soggetti coinvolti, sia privati che pubblici, ed è proprio a questi ultimi, in particolare, che è attribuito il compito di garantire la tutela dei diritti, salvaguardando l'ordine pubblico e sorvegliando sulla sicurezza nazionale.

È in questo contesto che si inserisce la Direttiva 2016/1148/UE, meglio conosciuta come Direttiva NIS[179], elaborata all'interno del "cantiere normativo" avviato nel 2016 dall'Unione Europea, quale opportunità per gli Stati membri di migliorare il proprio sistema.

La citata Direttiva NIS, quale risultato di un processo complicato conclusosi il 6 Luglio 2016, con termine di attuazione fissato al 9 Novembre 2018, rappresenta il *trait d'union* della regolazione pubblica nell'ambito della sicurezza informatica, essendo rivolta sia agli operatori pubblici che privati.

Essa costituisce un passaggio fondamentale per la costituzione di un sistema di sicurezza europeo, e tende all'armonizzazione delle legislazioni degli Stati membri, istituendo per ciascuno di essi l'obbligo di adottare una strategia nazionale e di supervisione sul raggiungimento di un elevato livello di sicurezza delle reti e dei sistemi informatici.

Grazie a tale Direttiva, resasi necessaria in un mercato digitale provato dai continui *cyberattacks* e *cybercrimes,* l' Unione Europea, attraverso regole puntuali e di coordinamento, assume un ruolo guida all'interno di un sistema che coinvolge pubblici e privati, le cui decisioni devono adeguarsi alle finalità previste; infatti «il compito degli Stati membri è quello di affinare le proprie "*cybersecurity*

[178] V. SARZANA DI S. IPPOLITO, *Informatica, Internet e diritto penale,* cit., 666 ss.
[179] NIS è l'acronimo di *Network and information Security.*

capabilities" e adottare una strategia nazionale unitamente a policy e misure regolatorie adeguate»[180].

In particolare, la Direttiva impone a ciascuno Stato di adottare le misure minime funzionali a garantire un livello minimo di sicurezza informatica e telematica, senza pregiudicare però l'eventuale loro volontà di applicare misure di sicurezza più elevata, conformemente al principio di sussidiarietà ed adeguatezza, secondo cui gli Stati membri possono scegliere di adottare o mantenere in vigore disposizioni volte a conseguire uno *standard* di sicurezza più elevato della rete e dei sistemi informatici.

I soggetti tenuti all'osservanza della Direttiva sono gli operatori di servizi essenziali[181] e i fornitori di servizi digitali attivi nei settori rispettivamente segnalati negli allegati II e III della stessa. I primi necessitano di essere identificati dagli Stati membri attraverso criteri espressamente previsti che devono essere applicati in modo coerente, diversamente dai secondi che sono indicati direttamente dalla direttiva per mezzo del duplice richiamo alla Direttiva 2015/1535.

Ad ogni modo, gli Stati membri sono tenuti a fornire alla Commissione un apposito elenco contenente l'informativa nazionale sulle misure volte a individuare gli operatori dei servizi essenziali, nonché il numero degli stessi e la lista dei servizi, ovvero tutti quei dati funzionali al processo di identificazione[182].

La Direttiva NIS si concentra su imprese e servizi "critici", sebbene gli Stati membri in sede attuativa possano decidere di estendere le previsioni anche a settori ulteriori, ampliando così il raggio d'azione ad ambiti non direttamente coinvolti

[180] V. MENSI, *La sicurezza cibernetica*, cit., 296.

[181] Cfr. *ivi*, 297: « [...]identificati, ancorché indirettamente, tramite il richiamo a una serie di criteri, con i soggetti pubblici o privati operanti nei settori dell'energia, dei trasporti, bancario, sanitario, nella fornitura e distribuzione di acqua potabile, nelle infrastrutture digitali o dei mercati finanziari qualora (i) forniscano un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali, (ii) la fornitura di tale servizio dipenda dalla rete e dai sistemi informativi; (iii) un incidente abbia effetti negativi rilevanti sulla erogazione di tale servizio».

[182] Cfr. *ivi*, 298: «Gli operatori dei servizi essenziali debbono essere stabiliti sul territorio nazionale; il che implica l'effettivo e reale esercizio di un'attività in loco anche mediante accordi commerciali, a prescindere dalla loro veste giuridica. Questo significa che uno Stato membro può avere giurisdizione su di essi non solo nel caso in cui il quartier generale sia stabilito sul suo territorio ma anche laddove operi una semplice filiale. Per quanto riguarda invece i fornitori di servizi digitali, è previsto che, nel caso in cui forniscano servizi all'interno dell'Unione europea, siano tenuti debbano designare un proprio rappresentante».

dalla stessa, in conformità con il principio di "armonizzazione minima" di cui all'art. 3 della stessa.

Al di là del già citato obbligo per gli Stati membri di adottare una strategia nazionale nell'ambito della sicurezza dei sistemi informatici e telematici, costituiscono ulteriori obiettivi della direttiva, come previsto dall'art. 1 della stessa, l'istituzione di un gruppo di collaborazione per sostenere e favorire la cooperazione strategica e lo scambio di informazioni, la creazione di una rete di gruppi di intervento per la sicurezza informatica c.d. CSIRT[183], l'imposizione dell'obbligo per gli Stati membri di istituire Autorità Nazionali competenti, punti di contatto unici e CSIRT con funzioni relative alla sicurezza della rete e dei sistemi informatici, e la previsione di obblighi di sicurezza e notifica per gli operatori di servizi essenziali e per i fornitori di servizi digitali.

Il legislatore europeo sottolinea la centralità della *governance* del rischio cibernetico, richiedendo che gli Stati acquisiscano le capacità tecniche e organizzative fondamentali per prevenire, individuare, contrastare e contenere i rischi e gli incidenti informatici, ragion per cui ogni Stato deve adottare un'adeguata strategia nazionale in materia, capace di individuare le finalità e gli interventi strategici da attuare in concreto; il piano strategico nazionale è altresì funzionale a predisporre un quadro di *governance* per realizzare gli obiettivi e le priorità definiti nella strategia.

Dunque, la Direttiva NIS incentiva la diffusione della "cultura della sicurezza", per prevenire e ridurre l'impatto di incidenti informatici, intesi quali eventi dannosi o pericolosi che pregiudicano la riservatezza, l'integrità, la disponibilità o l'autenticità dei dati memorizzati, divulgati o trattati, includendo nella nozione il fatto-reato in quanto tale.

È previsto l'obbligo per gli operatori dei servizi essenziali e per i fornitori di servizi digitali di notificare, senza indebito ritardo, all'autorità competente o al CSIRT, gli incidenti che abbiano: un impatto rilevante sulla "continuità dei servizi essenziali prestati", nel primo caso; un impatto sostanziale "sulla fornitura di un servizio", nel secondo caso. In quest'ultima situazione è contemplata la possibilità di informare il pubblico ad opera dell'autorità addetta o del CSIRT, a seguito di

[183] CSIRT è l'abbreviazione di *Computer security incident response team*.

consultazione con il fornitore di servizi digitali coinvolto. Talvolta, invece, può essere richiesto al fornitore di comunicare l'informazione al pubblico, e ciò accade generalmente nel caso in cui risulti utile sensibilizzare gli utenti, o laddove la diffusione dell'accaduto corrisponda ad esigenze di interesse pubblico. Spetta alle Autorità o ai CSIRT svolgere la valutazione nel merito circa l'eventualità della diffusione, in virtù dei possibili danni economici o reputazionali che ne derivano. È altresì consentito di effettuare una notifica su base volontaria degli incidenti ad opera di soggetti diversi da quelli suesposti, spettando alle autorità nazionali la relativa valutazione.

Laddove gli incidenti dovessero compromettere i dati personali è previsto l'intervento delle Autorità per la Privacy[184].

L'art. 21 della Direttiva NIS, quale generica disposizione circa la necessità di prevedere sanzioni, rimette agli Stati membri la specificazione di norme contenenti sanzioni effettive, proporzionate e dissuasive, da irrogare laddove le disposizioni nazionali attuative della Direttiva fossero violate, nonché l'adozione dei provvedimenti finalizzati alla loro applicazione[185].

La Direttiva NIS costituisce il referente normativo in base al quale è stato adottato il d.lgs. 18 maggio 2018, n. 65; ad essa vengono ricondotte anche numerose fonti ministeriali volte ad implementare la strategia nazionale di sicurezza cibernetica.

Sul piano dell'ordinamento interno il d.lgs. n. 65/2018 attuativo della Direttiva 1148/2016/UE, al pari di essa, è volto a sostenere la cultura di gestione del rischio e di segnalazione degli incidenti in campo cibernetico, ad affinare le capacità di *cyber* sicurezza del Paese e a consolidare la collaborazione a livello nazionale e comunitario, rafforzando il livello comune di protezione nell'Unione Europea[186].

Al fine di realizzare le suddette finalità, il decreto individua gli organi addetti ad adottare e attuare la strategia nazionale di *cybersicurezza*, definisce le

[184] MENSI, *La sicurezza cibernetica*, cit., 299 ss.

[185] V. DIRETTIVA (UE) 2016/1148, art. 21 del *Parlamento Europeo e del Consiglio*, in *www.eurlex.it*.

[186] SETOLA, ASSENZA, *Recepimento della Direttiva NIS sulla* cybersecurity *delle reti*, in *www. sicurezzaegiustizzia.com*, 20 gennaio 2019, 32 ss.

autorità NIS e il punto di contatto unico, prevede apposite linee guida per la sicurezza informatica e specifiche procedure di notificazione volontaria, e inserisce altresì un'appendice sanzionatoria nel caso di trasgressione degli obblighi imposti dal decreto.

La strategia nazionale di sicurezza cibernetica per la tutela delle reti e dei sistemi informatici nazionali viene adottata dal Presidente del Consiglio dei Ministri, sentito il CISR, ossia il Comitato interministeriale per la sicurezza della Repubblica. In essa sono indicati: gli obiettivi e le priorità per la protezione dei sistemi; un apposito quadro di *governance* funzionale a realizzare i citati obiettivi e ad indicare i ruoli e le responsabilità degli enti pubblici e degli altri soggetti; le misure di preparazione, riscontro e recupero compresa la cooperazione tra settore pubblico e privato; i programmi di formazione e sensibilizzazione relativi alla suddetta strategia; i piani di ricerca e sviluppo; un piano di valutazione dei rischi; l'elenco dei soggetti coinvolti nell'attuazione, le cui linee guida sono definite dal Presidente del Consiglio dei Ministri .

Il decreto designa le Autorità NIS indicando cinque ministeri, ciascuno responsabile in base alla propria competenza e allo specifico settore di riferimento: il Ministero dello sviluppo economico per il settore energia, nonché per quello delle infrastrutture e dei servizi digitali; il Ministero delle infrastrutture e dei trasporti per il campo del trasporto stradale, aereo, ferroviario e marittimo; il Ministero dell'economia e delle finanze per l'ambito bancario e dei mercati finanziari; il Ministero della salute per l'attività di assistenza sanitaria; il Ministero dell'ambiente per il settore fornitura e distribuzione di acqua potabile.

Tali autorità NIS hanno poteri ispettivi e di vigilanza relativamente all' adempimento degli obblighi di sicurezza delle reti e dei sistemi informativi. Laddove vi fossero violazioni degli obblighi di sicurezza e notifica, le suddette autorità hanno la facoltà di applicare sanzioni amministrative fino ad € 150.000[187].

Il Decreto ha altresì istituito il Punto di Contatto Unico presso il Dipartimento delle informazioni per la sicurezza, il quale svolge una funzione di collegamento per assicurare la collaborazione transfrontaliera delle autorità NIS

[187] SETOLA, ASSENZA, *Recepimento della Direttiva NIS sulla* cybersecurity *delle reti,* cit., 34.

con quelle competenti degli altri Stati membri, oltreché con il gruppo di cooperazione e con la rete CSIRT; esso partecipa ai lavori del gruppo di cooperazione formato dai rappresentanti degli Stati membri, della Commissione Europea e di ENISA, collaborando alla diffusione di *best practices* in materia.[188]

In osservanza dell'art. 21 della Direttiva NIS, il d.lgs. 65/2018 contiene un quadro articolato di sanzioni amministrative[189], rivolte agli operatori di servizi essenziali e ai fornitori di servizi digitali, le quali sono irrogate dalle rispettive autorità NIS competenti.

Sembra opportuno evidenziare la presenza di un'asimmetria tra le sanzioni imposte agli operatori dei servizi essenziali e quelle rivolte ai fornitori di servizi digitali, poiché solo nei confronti dei primi sono previste sanzioni amministrative per omessa adozione di misure di sicurezza. Tale scelta legislativa sembra contrastare con la direttiva NIS, che a tal proposito non effettua alcuna differenziazione, ragion per cui sarebbe corretto estendere anche ai fornitori dei servizi digitali le suddette sanzioni amministrative, in virtù del rilevante ruolo da essi svolto.

Per concludere dunque, il legislatore europeo ha inteso affermare la centralità dell'adozione di strategie e misure di *governance* del rischio cibernetico, sottolineando il ruolo decisivo svolto dalla *compliance*, quale strumento di garanzia della sicurezza informatica e cibernetica.

1.3.4 La legge n. 133/2019 di conversione del cd "Decreto Cybersicurezza"

La legge 18 novembre 2019, n. 133, di "Conversione in legge, con modificazioni, del decreto-legge 21settemnre 2019, n. 105, recante disposizioni urgenti in materia di perimento di sicurezza nazionale cibernetica" prevede l'istituzione di un perimetro di sicurezza nazionale cibernetica e di misure funzionali ad assicurare gli essenziali *standard* di sicurezza volti a ridurre i rischi.

Come si evince dal comma 1 dell'art. 1, la normativa è finalizzata a garantire «un **livello elevato di sicurezza delle reti,** dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori

[188] *Ivi*, 34 ss.

[189] Per approfondire le sanzioni amministrative v. *d.lgs. 18 maggio 2018, n.65*, art. 21, in *www. gazzettaufficiale.it*.

pubblici e privati aventi una sede nel territorio nazionale, **da cui dipende l'esercizio di una funzione essenziale dello Stato**, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e **dal cui malfunzionamento**, interruzione, anche parziali, ovvero utilizzo improprio, **possa derivare un pregiudizio per la sicurezza nazionale**»[190]**.**

Su proposta del CISR, la concreta formazione del suddetto perimetro e la definizione degli *iter* di notifica degli incidenti informatici interni allo stesso, nonché la determinazione delle misure di sicurezza, sono rimesse ad un Dpcm, previo parere delle Commissioni parlamentari competenti.

È altresì deferita ad un Regolamento, adottato anch'esso con Dpcm, la previsione di modalità e termini a cui pubblici e privati, inseriti nel perimetro di sicurezza nazionale cibernetica, devono adeguarsi per l'affidamento di forniture di beni, sistemi e servizi informatici e telematici[191].

In particolare, il Dpcm n. 131 del 30 luglio 2020 introduce il regolamento in materia di perimetro di sicurezza nazionale cibernetica, il quale contiene le modalità e i criteri di individuazione dei soggetti compresi nel succitato perimetro, obbligati al rispetto di specifiche prescrizioni, nonché i criteri utili a tali soggetti per la definizione e l'aggiornamento dell'elenco delle reti e dei servizi informatici di rispettiva competenza, da aggiornare con cadenza almeno annuale[192].

Il Dpcm in questione indica quindi, in base a determinati requisiti, le infrastrutture e gli strumenti informatici definiti "critici", in virtù degli effetti di una loro eventuale compromissione, richiedendo perciò un elevata protezione.

Più specificatamente, sul piano penale, in sede di conversione del Decreto Cybersicurezza è stata inserita, all' art. 1 comma 11, una nuova fattispecie a struttura "sanzionatoria"; la norma definisce differenti reati propri a dolo specifico, consistenti in falsità ideologiche "rilevanti" riferite alla disciplina extrapenale cui è

---

[190] Cfr. Decreto-Legge 21 settembre 2019, n.105, art 1, comma 1, convertito con modificazioni dalla L. 18 novembre 2019, n. 133 (in G.U. 20/11/2019, n. 272).

[191] IASELLI, *Sicurezza nazionale cibernetica: il decreto-legge coordinato in Gazzetta*, in *www.altalex.it*, 25 novembre 2019.

[192] FASI, Cybersecurity*: chi entra nel perimetro di sicurezza nazionale?,* in *www. fasi.biz*, 23 ottobre, 2020*; dpcm n.131 del 30 luglio 2020,* in (GU Serie Generale n. 261 del 21-10-2020), *www.gazzettaufficiale.it*.

ausiliaria, ed in un reato di omissione propria. Si tratta di delitti ascrivibili esclusivamente ai soggetti pubblici e privati con sede nel territorio nazionale, e ricompresi nel perimetro di sicurezza nazionale cibernetica.

La fattispecie penale considerata non tipizza le condotte delittuose, poiché rimanda agli obblighi giuridici dettagliatamente specificati in norme secondarie di attuazione[193].

Nel caso di violazione, seppur colposa, di precetti extrapenali, concernenti le misure di sicurezza, o la mancata comunicazione di informazioni importanti, finalizzate a favorire procedure ispettive e di controllo, sono previste sanzioni amministrative e interiettive. Tali illeciti amministrativi si differenziano rispetto alle fattispecie penali in ragione del fine specifico di intralciare le attività delle autorità competenti; inoltre, l'esistenza della clausola "salvo che il fatto costituisca reato" propria degli illeciti amministrativi precluderebbe la contestuale applicabilità di entrambe le tipologie di sanzioni[194].

È altresì opportuno rilevare che il comma 11-*bis* dell'art .1, inserito in sede di conversione del d.l. n. 105/2019 , ha introdotto nel catalogo dei reati presupposto di cui al d.lgs. n. 231/2001, le nuove fattispecie delittuose che se poste in essere implicano la responsabilità amministrativa dipendente da reato in capo all'ente: la modifica riguarda il comma 3 dell'art. 24-*bis* del d.lgs. n. 231/2001, concernente i delitti informatici, rispetto ai quali sono contemplate sanzioni pecuniarie e interdittive[195].

Per concludere, alla luce dei più recenti sviluppi tecnologici, tra i quali è meritevole di menzione la rete 5G, tale intervento normativo assume una rilevanza determinante nel panorama nazionale, contribuendo a consolidare e ad accrescere la tutela della *cybersecurity* nel più ampio contesto sovranazionale.

---

[193] PICOTTI, VADALÀ, *Sicurezza cibernetica: una nuova fattispecie delittuosa a più condotte con estensione della responsabilità degli enti*, in *Sist. pen.*, 5 dicembre, 2019, che richiama FLOR, Cybersecurity *ed il contrasto ai* cyber-attacks *a livello europeo*, cit., 443 ss.

[194] *Ibidem*.

[195] *Ibidem*.

CAPITOLO II

FINANCIAL CYBERCRIMES: LE TRUFFE *ON-LINE*

2.1 La tutela penale del patrimonio nel *cyberspace*. Rilievi introduttivi.

La diffusione delle tecnologie informatiche e telematiche e le conseguenti forme di interconnessione globale fra sistemi hanno notevolmente inciso sulle relazioni sociali, incrementando le funzionalità dei servizi e degli strumenti digitali, e modificando così il tradizionale svolgimento delle dinamiche quotidiane.

Come si evince dalla trattazione del precedente capitolo, infatti, agli innumerevoli vantaggi in punto di innovazione, propri della digitalizzazione, si affiancano gli aspetti critici della nuova dimensione, rappresentati da inedite forme di aggressione e dal diffuso – e già citato – fenomeno della criminalità informatica, e più in generale cibernetica, capace di pregiudicare qualunque sfera di contatto e di ledere diversi beni giuridici, coinvolgendo differenti settori[196]. In tale contesto i soggetti sono esposti al pericolo di continue interferenze e di incessanti offese ai suddetti beni giuridici, tra i quali, per quel che concerne il presente elaborato, assume rilevanza il patrimonio, quale comune interesse meritevole di tutela penale nelle truffe *on-line*.

A tal proposito, non deve essere trascurata la diversità di valore esistente tra le condotte materiali, tipiche dei reati tradizionalmente commessi, e le condotte realizzate nell'ambiente digitale, ovverosia perpetrate in rete mediante l'impiego degli strumenti telematici, poiché da queste ultime deriverebbe una lesione patrimoniale ancor più incisiva di quella risultante dai comportamenti materialmente realizzati[197]. La nascita della dimensione tecnologica ha posto, infatti, la necessità di ridefinire la tutela penale degli interessi patrimoniali degli utenti tenendo conto della rapidità e dell'astrattezza, nonché di tutte le altre caratteristiche proprie delle modalità offensive tipiche delle condotte digitali realizzate nel cyberspazio, luogo contraddistinto da dematerializzazione, anonimato, atemporalità e aterritorialità. Proprio tali peculiarità, infatti,

[196] V. CUOMO, RAZZANTE, *La nuova disciplina dei reati informatici*, Torino, 2009, 3.
[197] Sul punto v. SCOPINARO, *Internet e reati contro il patrimonio*, Torino, 2007, 225.

ripercuotendosi sul contenuto offensivo degli elementi costitutivi del reato, hanno imposto una rivalutazione della concezione e della protezione patrimoniale nel cyberspazio[198]. Le suddette caratteristiche, inoltre, hanno facilitato ed incentivato il compimento di reati in rete, tra cui le truffe *on-line*, ad opera dei c.d. "delinquenti informatici".

Tuttavia, per completezza espositiva e per meglio comprendere il significato attribuito al patrimonio, quale bene giuridico penalmente tutelato nell'ambito dei *cybercrimes*, nonché per facilitare la successiva disamina del tema, sembra opportuno, in via preliminare, assumere un approccio più ampio e generalizzato dell'argomento in questione, prendendo le mosse dalle concezioni tradizionali della nozione patrimoniale e introducendo le tipicità proprie della categoria dei reati informatici contro il patrimonio.

Nel corso del tempo si è manifestata la proliferazione delle opportunità volte ad ottenere profitto per mezzo dello sfruttamento delle operazioni eseguite dai sistemi operativi. Sin dai primi anni Settanta del secolo scorso, infatti, i sistemi informatici, oggetto di abuso da parte dei criminali, si sono mostrati come semplici bersagli e vantaggiosi strumenti di indebito arricchimento, risultando altresì evidente l'inadeguatezza delle norme penali esistenti a contrastare tale situazione.

In altri termini, le specifiche modalità esecutive proprie delle nuove forme aggressive, consentite ed agevolate dalle innovazioni tecnologiche, risultavano differenti da quelle abituali, seppur offensive dei medesimi beni giuridici, tanto da non poter essere ricondotte alle fattispecie incriminatrici poste a tutela di quegli

[198]Cfr. SCOPINARO, *Internet e reati contro il patrimonio*, cit., 225: «La differenza di valore fra il comportamento realizzato nell' ambiente materiale e quello posto in essere nel contesto digitale non si manifesta solo nella questione che concerne la possibilità di ravvisare nel fatto gli elementi previsti dalle fattispecie tipiche formulate per reprimere fatti materiali ma si ripercuote sul contenuto offensivo degli elementi costituivi del reato, imponendo una rivisitazione della tradizionale concezione del patrimonio, così come essa si traduce nella configurazione astratta delle norme. La configurazione della fattispecie diretta a punire un fatto informatico lesivo del patrimonio individuale deve tenere conto del fatto che il nuovo comportamento è caratterizzato da elementi di valore propri ed è privo degli elementi di valore che nelle fattispecie non informatiche, sono legati alla materialità delle cose»; in argomento v. anche CARMONA, *I reati contro il patrimonio*, in FIORELLA (a cura di), *Questioni fondamentali della parte speciale del diritto penale. Estratto ad uso degli studenti Università degli studi "Sapienza"*, 3ª ed., Torino, 2019, 11: «Dunque, al legislatore penale non interessa tanto la lesione del bene patrimonio[…], quanto il modo con il quale il bene viene leso. È proprio attraverso la individuazione della modalità della condotta che si determina il livello di offesa penale[…]».

stessi beni, in osservanza del divieto di applicazione analogica delle norme penali[199].

Inoltre, la natura transnazionale del fenomeno ha immediatamente evidenziato l'esigenza, nonché l'urgenza, di un intervento repressivo, possibilmente uniforme, per scongiurare la creazione dei c.d. "paradisi informartici". A tal proposito un primo rilevante contributo è stato fornito dalla Raccomandazione del Consiglio d' Europa n. R(89), contenente un catalogo di condotte di abuso dell' informatica oggetto di interesse da parte dei Paesi coinvolti, indicando nella "lista minima" i comportamenti che gli stessi sono invitati a reprimere servendosi, oltreché del tradizionale strumento della pena, anche di interventi legislativi *ad hoc*, nei quali figurano le predette aggressioni al patrimonio, e nella "lista facoltativa" le condotte solo eventualmente incriminabili, ossia punibili a discrezione dei singoli Stati in base ad un'apposita valutazione circa la meritevolezza della pena[200].

In Italia, per quel che concerne, in particolare, i reati informatici contro il patrimonio inseriti nel Codice penale, assume rilevanza la Legge n. 547/1993, alla quale, più in generale, si deve l'ingresso di specifici reati informatici nell'ordinamento nazionale, garantendo così la repressione penale della maggioranza dei comportamenti antigiuridici indicati nella Raccomandazione n. R(89). Più precisamente, a tutela del patrimonio, la suddetta Legge n. 547 del 1993 ha previsto le nuove fattispecie di frode informatica, *ex* art. 640-*ter* c.p., e di danneggiamento dei sistemi informatici o telematici, *ex* art. 635-*bis* c.p[201]., in aggiunta alle tipiche norme sulla truffa e sul danneggiamento. È stata inoltre inserita una specifica disposizione, all'art. 615-*quinquies* c.p.[202], sulla diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o

[199] Sul punto v. PECORELLA, *I reati informatici contro il patrimonio*, in PULITANÒ (a cura di), *Diritto penale. Parte speciale. Volume II. Tutela penale del patrimonio*, Torino, 2013, 271.

[200] *Ivi*, 271 s.

[201] Cfr. PECORELLA, *I reati informatici contro il patrimonio*, cit., 274. Sul punto è altresì necessario precisare che la Legge di ratifica della Convenzione di Budapest n. 48/2008 ha ridefinito la fattispecie di danneggiamento informatico, sdoppiandola in base al diverso oggetto della condotta, il quale può riferirsi ai dati – art. 635-*bis* c.p. – ovvero ai sistemi informatici – art. 635-*quater* –, prevedendo inoltre due ulteriori figure di reato aventi ad oggetto i dati – art. 635-*ter* – e i sistemi – art. 635-*quinquies* – di pubblica utilità.

[202] Disposizione riformulata dalla Legge di ratifica della Convenzione di Budapest n. 48/2008, che ha notevolmente ampliato l'ambito di operatività della norma originaria: cfr. *Ivi*, 275 e 292.

interrompere un sistema informatico o telematico, seppur impropriamente collocata tra i delitti contro l'inviolabilità del domicilio[203].

Ad ogni modo, sembra opportuno puntualizzare che forme di aggressione "informatica" ai beni altrui sono altresì contemplate come potenziali modalità di realizzazione di reati che ledono direttamente beni differenti dal patrimonio individuale, come, ad esempio, nel caso dell'accesso abusivo ad un sistema informatico o telematico *ex* art. 615-*ter*, «contemplato tra i delitti contro l'inviolabilità del domicilio e del quale il danneggiamento dei beni informatici altrui costituisce una circostanza aggravante»[204].

Infine, senza voler entrare nel merito delle singole ipotesi, è bene aggiungere che nel quadro generale delle disposizioni funzionali a contrastare le aggressioni informatiche al patrimonio rientrano l'art. 493-*ter* c.p.[205], relativo all'indebito utilizzo e falsificazione di carte di credito e di pagamento, e le previsioni in tema di *cyberlaundering* e *cyber self-laundering*, quali forme di sfruttamento delle nuove tecnologie finalizzate al riciclaggio e all'autoriciclaggio di denaro sporco in rete.

Dunque, l'indagine relativa alle offese al patrimonio individuale poste in essere sfruttando il contesto digitale si rende indispensabile in ragione del fatto che si riferisce ad una categoria di reati che assume una posizione centrale nel quadro dei reati informatici in generale, trattandosi di un fenomeno manifestatosi sin dal primo impiego della tecnologia, e profondamente accentuatosi con la comparsa del *Web*[206]. Nell'ambito di questa trattazione, pertanto, il bene giuridico in base al quale devono essere individuati i fatti potenzialmente idonei ad assumere rilevanza penale è il patrimonio individuale, il quale rappresenta uno degli interessi giuridicamente rilevanti la cui tutela è richiamata nei reati informatici, in cui l'informatica, appunto, costituisce un elemento di rilievo fattuale[207].

Deve essere ulteriormente specificato che, nel corso del tempo, l'elemento informatico caratteristico di questa tipologia di reati, lesivi del patrimonio, è

---

[203] *Ivi*, 273 s.

[204] Cfr. PECORELLA, *I reati informatici contro il patrimonio,* cit., 274.

[205] In passato il delitto di indebito utilizzo e falsificazione di carte di credito e di pagamento era previsto dall'art. 12 della legge n. 197 del 1991, successivamente sostituito dall'art. 55, comma 9, del D.lgs. n. 231/2007, il quale è stato a sua volta abrogato dall'art. 493-*ter*, inserito nel Codice penale con il D.lgs. n. 21/2018, attuativo della delega contenuta nella Legge n. 103/2017.

[206] In argomento v. SCOPINARO, *Internet e reati contro il patrimonio,* cit., 1 s.

[207] *Ivi*, 9.

mutato, determinando una variazione nelle modalità di realizzazione concreta del fatto penalmente rilevante, mantenendosi costante, al contrario, l'offesa al bene individuale patrimoniale; infatti, mentre in passato i reati informatici erano commessi sfruttando per lo più un collegamento di rete di tipo locale, attualmente il compimento di specifici reati informatici, o meglio cibernetici, contro il patrimonio, presuppone l'esistenza di un'interconnessione globale fra sistemi, basandosi non di rado su operazioni di vendita telematica di beni e servizi, favorite dalla nascita del *Web* e del commercio elettronico. Dunque, tali tipi di crimini si realizzano *on-line*, determinandosi così una tendenziale indipendenza del *server* o del sistema operativo di partenza rispetto al luogo in cui l'agente pone in essere il comportamento antigiuridico, ovvero alla posizione assunta in rete dai soggetti coinvolti.

In ragione delle caratteristiche proprie della rete possono essere compiute *on-line* anche le attività preliminari alla concretizzazione del reato, ravvisandosi altresì la possibilità di stabilire una concatenazione fra reati, in virtù degli automatismi e della permanenza delle connessioni fra i sistemi. Vi sono, peraltro, eventualità in cui il predetto collegamento fra i sistemi operativi può comportare la definizione di reati alquanto diversi tra loro, potendosi produrre effetti lesivi di beni giuridici differenti su ciascuno dei sistemi connessi[208].

Come preannunciato, al fine di cogliere il reale valore che assume il bene giuridico in esame nella nuova dimensione rappresentata dal cyberspazio, non si può prescindere dal considerare i tradizionali profili sostanziali propri del diritto penale, validi perciò non solo nella realtà materiale, bensì anche in quella cibernetica.

Dunque, più in generale, per quel che riguarda i delitti contro il patrimonio, essi sono previsti nel Titolo XIII del libro II del Codice penale[209], all'interno del

---

[208] *Ivi*, 9 s. e 18 ss.

[209] V. ANTOLISEI, *Manuale di diritto penale. Parte speciale*, Vol. I, 16 ª ed., Milano, 2016, 400 s.: per completezza, si precisa che il codice vigente distingue i delitti patrimoniali in due classi, a seconda del fatto che siano realizzati tramite violenza a cose o persone, ovvero tramite frode. Nel secondo gruppo, riconducibile al Capo II del Titolo XIII del libro II, sono ricompresi i reati d'interesse quali la truffa *ex* art. 640 c.p. e la frode informatica *ex* art. 640-*ter* c.p. Ad ogni modo, si tratta di una distinzione discutibile poiché si basa sull' errata premessa di fondo secondo cui la criminalità può assumere o la forma della violenza o quella della frode, non tenendo presente che in numerosi fatti antigiuridici non sono ravvisabili né la violenza né la frode.

quale si distinguono perciò anche fattispecie di reato che incriminano, o a cui possono essere ricondotte, numerose condotte informatiche e cibernetiche, come quelle oggetto del presente elaborato, in quanto offensive del patrimonio, quale comune bene giuridico tutelato dalla suddetta categoria di reati. Tuttavia, è bene sottolineare che le figure incriminatrici presenti nel suddetto titolo non esauriscono il catalogo dei delitti contro il patrimonio, poiché anche in altri titoli si ravvisano figure criminose che comunque ledono interessi patrimoniali, seppur talvolta unitamente ad altri interessi; allo stesso modo, può affermarsi che i reati inclusi nel titolo in esame potrebbero non risultare esclusivamente offensivi del bene giuridico patrimoniale, potendo pregiudicare anche ulteriori valori meritevoli di tutela penale[210].

È essenziale, a questo punto della trattazione, esaminare la complessa nozione di patrimonio, comunemente inteso come l'insieme delle attività e delle passività che si riferiscono ad un soggetto. In termini strettamente giuridici il patrimonio è solitamente definito come il «complesso dei rapporti giuridici, economicamente valutabili, che fanno capo ad una persona»[211].

Secondo i privatisti, più che di un mero insieme di cose o beni, si tratta di un complesso di rapporti, ovverosia di diritti e di obblighi, e questi sottolineano che siffatti rapporti devono riguardare cose o entità provviste di un valore economico e, pertanto, devono essere quantificabili in denaro.

Secondo Autorevole dottrina[212], il concetto elaborato dai cultori del diritto privato è valido, seppur con una notevole precisazione, anche per il diritto penale; il criterio del valore economico e pecuniario restrittivamente inteso dalla dottrina privatistica, difatti, non può essere condiviso dai penalisti. Più esattamente, nel diritto penale, come in quello privato, i beni ritenuti, secondo la comune opinione, economicamente irrilevanti sono considerati tendenzialmente estranei al patrimonio, ma nell'ambito penale, diversamente da quello privato, un oggetto che assume valore di affezione per chi lo possiede, sebbene sprovvisto di valore di scambio, è da ritenersi incluso nel patrimonio. In altri termini, ai fini penalistici, le

[210] In tal senso ANTOLISEI, *Manuale di diritto penale*, cit., 374 s.
[211] In tal senso ANTOLISEI, *Manuale di diritto penale*, cit., 377.
[212] Secondo quanto sostenuto da ANTOLISEI, *Manuale di diritto penale*, cit., 377.

cose che, seppur prive di valore economico, hanno un valore sentimentale per il soggetto che le possiede devono essere considerate parte della sfera patrimoniale[213].

Rientrano dunque nella suddetta nozione tutti i diritti reali, i diritti di obbligazione, ed il possesso; qualche incertezza, risolta in senso positivo, si è manifestata relativamente alle aspettative, ossia alle situazioni che contemplano la possibilità di un profitto lecito, risultando, in definitiva, anch'esse ricomprese[214].

Al contrario, non sembrano essere incluse nel patrimonio la capacità produttiva, le pretese prive di fondamento giuridico e quelle antigiuridiche.

Da quanto finora esposto, emerge chiaramente che la discussa questione circa la natura giuridica o economica del patrimonio, quale oggetto della tutela penale, debba concludersi in favore della prima. Del resto, un approccio prettamente economico conduce ad esiti inaccettabili[215].

Dunque, si deve affermare che l'offesa al patrimonio, quale fondamento dei delitti in esame, «si verifica tutte le volte che viene violato un obbligo di non ingerenza relativo ad un rapporto patrimoniale e, precisamente, ad un rapporto che abbia come proprio oggetto o un valore economico o un valore di affezione»[216].

---

[213] *Ivi*, 377 s.

[214] *Ivi*, 378; inoltre l'Autore ritiene che «anche i valori posseduti in contrasto col diritto fanno parte del patrimonio, dato che, entro certi limiti, il possesso di essi […], come quasi concordemente si ammette, è tutelato dall'ordinamento giuridico».

[215] Cfr. ANTOLISEI, *Manuale di diritto penale*, cit., 379: in base alla concezione economica «dovrebbe considerarsi insussistente il furto nel caso che taluno, impossessandosi della cosa mobile altrui, lasci sul posto un oggetto di valore almeno equivalente.

[216] *Ivi*, 379 ss. ove si legge: «è noto che l'ordinamento giuridico in taluni casi e per certi scopi considera il patrimonio come una unità organica […] e lo tratta come un sol tutto, indipendentemente dai diritti che lo compongono. […]. La dottrina italiana è concorde nel ritenere che, nel campo penale, il patrimonio non è mai tutelato come un'entità autonoma, come universalità dei diritti che fanno capo ad una persona. Si dice generalmente che, ai fini della protezione penale, il patrimonio, di fronte all' attività del reo che lo aggredisce, si discioglie, risolvendosi nei singoli rapporti dai quali risulta, ed in sostanza nelle singole cose e nei diritti che lo costituiscono. Malgrado l'unanimità dei consensi, quest'opinione non può ritenersi fondata, essendo inesatta la premessa da cui parte, e cioè l'affermazione che la legge penale non offra alcuna figura delittuosa che sia preordinata alla tutela dell'intiero patrimonio. Tale affermazione è in contrasto con le risultanze a cui è pervenuta la dottrina straniera e specialmente quella germanica, la quale ha posto giustamente in rilievo che, se nella maggior parte dei casi i reati patrimoniali sono diretti contro singoli diritti determinati preventivamente (furto, appropriazione indebita, rapina, usurpazione, danneggiamento, ecc.), ve ne sono parecchi che offendono il patrimonio nella sua totalità. Tale è la truffa, l'estorsione, l'insolvenza fraudolenta, la circonvenzione delle persone incapaci, l'usura, ecc. Senza dubbio anche questi delitti nei casi concreti possono dirigersi di regola contro dati diritti, ma, a differenza dei delitti precedenti, i diritti offesi non sono individuati nelle fattispecie legali».

È bene precisare, inoltre, che tra le diverse definizioni di patrimonio elaborate dalla dottrina penalistica[217] la più apprezzata è quella – c.d. "giuridico-

[217] Per approfondire sul punto v. CARMONA, *I reati contro il patrimonio*, cit., 2 ss., secondo cui: la disamina relativa ai delitti contro il patrimonio non può che fondarsi sulla definizione dell'oggettività giuridica comune alle differenti figure incriminatrici, rievocando le varie nozioni di patrimonio condivise dalla dottrina penalistica nel corso del tempo. A tal proposito è bene premettere che sul piano generale la concezione tecnico-giuridica di patrimonio, di matrice civilistica, presenta peculiarità che possono non risultare tutte significative nel campo penale. «Se è certo, infatti, che fra il concetto generale di patrimonio, valido per tutto l'ordinamento giuridico, e il bene giuridico penale vi sia una notevole coerenza, anzi un'estesa coincidenza di oggetto, non può negarsi, del pari, come dal concetto generale, di matrice civilistica, vada espunto tutto quanto non sia utile agli scopi tipici dell'intervento penale (o, viceversa, aggiunto, quanto sia necessario considerare da questo punto di vista)».

Ad ogni modo, si constata che anche un'adeguata definizione del concetto di patrimonio non è sempre capace di risolvere proficuamente ogni questione sollevata dalle diverse figure delittuose. «Le ragioni sottese a tale limite devono essere individuate da un lato nel ruolo decisivo che le modalità di condotta rivestono rispetto alla determinazione dell'offesa, dall'altro nell'incidenza che le diverse esigenze politiche, storicamente emerse, hanno avuto nella formazione e modificazione delle specifiche ipotesi di reato. Ciò non deve, però, far rinunciare alla ricerca di concetti generali validi per il maggior numero possibile di fattispecie, allo scopo di mantenere una visione d'insieme indispensabile a cementare le singole figure delittuose in un sistema».

Sono state sviluppate dalla dottrina penalistica tradizionale differenti concezioni del patrimonio: la tecnico-giuridica, l'economica, l'economico-giuridica e la giuridico-funzionale.

La prima, c.d. "tecnico-giuridica", definisce il patrimonio come «il complesso dei diritti soggettivi patrimoniali che fanno capo ad una persona». In ragione dell'origine civilistica di tale concezione tecnico-giuridica, vi è il dubbio circa l'opportunità di adattare efficacemente la stessa alle esigenze proprie del diritto penale, senza una preliminare apposita valutazione delle finalità pratiche di tutela delle singole fattispecie. Oggigiorno, la suindicata concezione non sembra condivisibile, poiché «[…]lo schema tipicamente civilistico esclude dalla rilevanza penale, e dunque dai profili dell'offesa, ogni relazione puramente fattuale e, comunque, ogni situazione non definibile come diritto soggettivo (ad esempio, le aspettative). In tale prospettiva, restringendo l'area della tutela penale ai rapporti di carattere patrimoniale che vestano gli abiti del diritto soggettivo, rimarrebbero al di fuori del concetto di patrimonio penalmente rilevante tutte le situazioni di fatto che legano un soggetto ad una cosa e che pur potrebbero essere meritevoli di protezione».

La seconda concezione, c.d. "economica", consente di andare oltre i limiti propri della nozione tecnico-giuridica, intendendo il patrimonio come il «complesso dei beni economicamente valutabili appartenenti in forza di un diritto o per un rapporto di fatto ad una persona». Dunque, sulla base di tale approccio, il patrimonio risulta composto esclusivamente da beni economicamente valutabili, ed appartenenti ad un soggetto in ragione di un diritto o di un rapporto di fatto. «La prospettiva della "valutazione economica" dei beni si presta ad insuperabili obiezioni. In primo luogo, poiché l'unica aggressione penalmente rilevante diviene quella che comporta una reale diminuzione economica, si permetterebbe all'autore di compensare la perdita provocata con altro equivalente economico, sottraendosi, così, allo spettro di incriminazione della fattispecie, pur avendo il fatto inciso negativamente sul titolare del rapporto aggredito per l'impossibilità, ad esempio, di usare la cosa sottratta[…]». Perciò, in base ad una simile costruzione, nei casi in cui non si dovesse verificare una *deminutio patrimoni* economica non si potrebbe configurare alcun danno al bene giuridico tutelato. Tale concezione, basata unicamente sul valore economico dei beni, conduce a risultati giuridici inammissibili, poiché non protegge penalmente tutte quelle situazioni che, seppur rilevanti sotto il profilo affettivo, o in base ad un valore d'uso, risultano sprovviste di valore di scambio. Inoltre, accogliendo tale impostazione, si dovrebbero considerare parte del patrimonio «tutti i beni, economicamente valutabili, per la sola circostanza di appartenere di fatto ad una persona, senza che si richieda nessuna ulteriore qualificazione»; oltretutto, risulterebbero meritevoli di tutela anche i beni introdotti illegalmente nella sfera giuridica di una persona, in ragione del suindicato rapporto di fatto.

funzionale" – che concepisce lo stesso come l'insieme dei rapporti giuridici facenti capo ad una persona, aventi ad oggetto cose dotate di funzione strumentale, volte ad appagare i bisogni materiali o spirituali[218]. Si tratta di una concezione personalistica che, riferendosi a rapporti giuridici con valore non solo economico ma anche affettivo, attribuisce un rilievo primario alla tutela della personalità individuale, coerentemente con i principi costituzionali – *ex* artt. 2, 3, 41 e 42 Cost. – che privilegiano in modo assoluto l'individuo e la sua dignità, e dunque la sua completa realizzazione nella società, al di là delle singole condizioni economiche di ciascun soggetto[219]; essa, infatti, riflette il particolare rilievo che il concetto di patrimonio assume nella realtà esistenziale del singolo[220]. Al contrario, se non si ricomprendesse nella suddetta nozione anche il valore di affezione, escludendo quindi dalla tutela penale le situazioni prive di contenuto economico, vi sarebbe una limitazione delle garanzie costituzionali, in base alle quali è doveroso tutelare nel

La concezione "economico-giuridica" considera il patrimonio come «il complesso dei rapporti giuridici […] economicamente valutabili che fanno capo ad una persona». In tale definizione viene sottolineata la qualificazione giuridica del rapporto con la cosa, la quale rende intrinsecamente lecito il suddetto rapporto, precludendo così la possibilità di includere nel patrimonio relazioni di natura illecita. Ciononostante, la suddetta concezione non sembra soddisfacente nella condizione in cui limita la tutela ai rapporti giuridici puramente economici, non includendo quelli a contenuto affettivo, ai quali, al contrario, deve essere riconosciuta una funzione essenziale nella determinazione della nozione di patrimonio penalmente tutelato.

«Una interpretazione attuale del diritto penale liberale, centrato sulla tutela di beni giuridici attraverso la selezione delle specifiche condotte di aggressione, non può essere compiuta se non attraverso una lettura costituzionale del bene e delle tecniche di normazione usate per proteggerlo». Dunque, il concetto di patrimonio, quale bene giuridico tutelato, deve essere definito nel rispetto dei principi costituzionali – *ex* artt. 2, 3, 41 e 42 Cost. – che fissano al centro del sistema la salvaguardia della persona e la sua dignità, pertanto non sembra condivisibile la concezione economico-giuridica di patrimonio che si limiti all'insieme dei rapporti giuridici solo se economicamente valutabili, escludendo così dalla tutela penale la lesione di rapporti giuridici a contenuto meramente affettivo.

È stata avanzata una quarta definizione di patrimonio, c.d. "giuridico-funzionale", secondo la quale esso «è costituito dal complesso dei rapporti giuridici facenti capo ad una persona aventi per oggetto cose dotate di funzione strumentale a soddisfare bisogni materiali o spirituali». In tal caso, in osservanza dei succitati principi costituzionali, sono introdotti nella nozione patrimoniale i rapporti a valore affettivo accanto a quelli a valore economico. Ad ogni modo, il rischio di ampliare eccessivamente la tutela penale a causa della potenziale esasperazione del succitato valore affettivo della cosa, nel caso in cui vi fosse una smisurata valorizzazione della mera sensibilità personale della vittima, è sventato dalla stessa definizione giuridico-funzionale di patrimonio, la quale non prevede espressamente il riferimento a rapporti con valore sentimentale, ma specifica che il rapporto deve avere ad oggetto cose con funzione strumentale a realizzare esigenze d natura materiale o spirituale.

[218] In argomento v. CARMONA, *I reati contro il patrimonio*, cit., 6.

[219] *Ivi*, 5 e 7.

[220] *Ivi*, 8.

modo più ampio possibile l'individuo, la cui personalità si estrinseca, perciò, anche, e specialmente, in virtù di situazioni sprovviste di valore di scambio[221].

Inoltre, è bene precisare che nell'impostazione "giuridico-funzionale", al fine di stabilire se un rapporto giuridico possa essere considerato parte del patrimonio, più che il contenuto economico o affettivo, rileva l'effettiva funzione strumentale finalizzata a soddisfare le necessità del soggetto interessato[222].

Quest'ultima nozione di patrimonio, sviluppata dalla dottrina penalistica, è considerata attualmente condivisibile, e sembra agevolmente adattabile alle nuove esigenze dettate dall'evoluzione tecnologica, assicurando così la tutela del suddetto bene giuridico in tutti i casi in cui se ne ravvisi il rischio di aggressione, anche in presenza di alterazioni patrimoniali di modesta entità.

In aggiunta a quanto già detto, per completezza, si ritiene di dover identificare il significato proprio delle nozioni di "danno" e "profitto", in ragione del rilievo che questi assumono nell'ambito dei delitti – anche informatici o cibernetici – contro il patrimonio.

Il danno è un requisito esplicito di alcune figure criminose e comunque implicito di tutti i reati patrimoniali, poiché i fatti descritti in ciascuna fattispecie possono essere sottoposti a pena solo se recano un danno giuridicamente rilevante. Si tratta di un danno patrimoniale, poiché il bene giuridico penalmente tutelato è il patrimonio; tale danno patrimoniale consiste nella c.d. "*deminutio patrimonii*", ovverosia nella riduzione dell'insieme dei valori che costituiscono il patrimonio, e rappresenta «un'alterazione patrimoniale sfavorevole (o in peggio) del rapporto fra gli elementi attivi e gli elementi passivi del patrimonio»[223].

Il suddetto danno deve essere valutato con criteri oggettivi, ma tenendo comunque in considerazione le peculiarità del caso concreto e i rapporti patrimoniali del soggetto coinvolto. Ad ogni modo, poiché, come già detto, la nozione patrimoniale si riferisce non solo ai rapporti giuridici con valore economico, ma anche a quelli con valore affettivo, è possibile affermare che il

---

[221] V. CARMONA, *I reati contro il patrimonio,* cit., 8: «[…]avendo di mira la tutela della personalità individuale, dall'adesione alle tesi economiciste si farebbe discendere in sede penale un vuoto di tutela che non può non riflettersi negativamente sulla personalità dell'individuo».

[222] In argomento v. SCOPINARO, *Internet e reati contro il patrimonio,* cit., 26.

[223] Cfr. ANTOLISEI, *Manuale di diritto penale,* cit., 388.

danno patrimoniale non coincide esattamente con il danno economico: infatti il primo include senz'altro il secondo, ma presenta un'estensione più ampia, ricomprendendo anche i rapporti sprovvisti di valore di scambio[224].

A proposito del profitto, la significatività del concetto nell'ambito dei delitti contro il patrimonio dipende dal fatto che nella gran parte delle norme incriminatrici è richiesto che l'azione sia realizzata a scopo di profitto. Per di più, in alcuni reati, il conseguimento del suddetto vantaggio rappresenta una vera e propria condizione d'esistenza, come nel caso della truffa o della frode informatica.

Secondo la più ampia nozione di profitto condivisa dal diritto italiano, «non è profitto soltanto il vantaggio economico e, più in genere, l'incremento del patrimonio, ma qualunque soddisfazione o piacere che l'agente si riprometta dalla sua azione criminosa. Senza dubbio, nella generalità dei casi il profitto consiste in un'utilità pecuniaria ma ciò non è indispensabile: l'utilità può essere anche di natura diversa»[225]. Inoltre, nella maggioranza delle norme incriminatrici in cui si parla di profitto appare l'aggettivo "ingiusto", indicando dunque che, ai fini della sussistenza del reato, è richiesto che tale vantaggio abbia il carattere dell'ingiustizia. Nell'ambito del presente elaborato è bene riferirsi al profitto patrimoniale, considerandolo ingiusto solo se non è minimamente tutelato, né direttamente né indirettamente, dall'ordinamento giuridico. La nozione di profitto è sempre affiancata dall'espressione "per sé o per altri" nell' intento di sottolineare che «la responsabilità penale sussiste anche se la lesione del patrimonio è stata effettuata dal soggetto per avvantaggiare una terza persona»[226].

Al fine distinguere i reati offensivi del patrimonio, perpetrati anche nel cyberspazio, occorre sottolineare i tratti essenziali propri dell'intervento penale in tema di tutela patrimoniale individuale e definire i modelli normativi astratti assunti nell'ambito dell'apposito titolo del Codice penale.

Per quel che concerne gli elementi costituitivi dei delitti contro il patrimonio, assumono un ruolo decisivo le concrete modalità di svolgimento del

---

[224] *Ibidem*.

[225] Cfr. ANTOLISEI, *Manuale di diritto penale,* cit., 389 s., il quale precisa, inoltre, che il profitto è per sua natura relativo.

[226] Cfr. *Ivi*, 391 s.; inoltre «[…]la temporaneità o transitorietà del profitto è irrilevante. Anche un vantaggio temporaneo o provvisorio, infatti, rappresenta un profitto».

fatto; si attribuisce all'interesse patrimoniale, quale comune bene giuridico protetto, «una funzione unitaria di caratterizzazione delle singole fattispecie»[227], e si realizza per mezzo della tipizzazione della condotta «la frammentazione dell'intervento penale»[228].

È opportuno specificare, infatti, che si ravvisano due differenti modelli di lesione al patrimonio: il primo in cui il soggetto agisce autonomamente, escludendo la cooperazione altrui «artificiosamente oppure violentemente ottenuta»[229]; il secondo in cui l'agente approfitta della suddetta collaborazione per conseguire un profitto e causare un danno[230]. In quest'ultima ipotesi la cooperazione di un soggetto «è componente della fattispecie tipica, elemento causalmente collegato come risultato della condotta dell'agente e come antecedente al profitto che l'agente si procura con danno per il soggetto passivo»[231].

La struttura tipica delle fattispecie di cooperazione artificiosa richiede necessariamente la collaborazione di un altro individuo – «sia egli solo il soggetto passivo della condotta o anche il soggetto passivo del reato»[232] – per compiere il reato offensivo del patrimonio; in tal caso, però, si ledono inevitabilmente anche altri beni giuridicamente tutelati e riferibili al soggetto che subisce la condotta, come ad esempio la libertà morale o di autodeterminazione, l'integrità fisica e la fiducia individuale. Anche nelle aggressioni unilaterali può verificarsi una condotta plurioffensiva, ma tale molteplice pregiudizio è solo eventuale, poiché, a seconda dei casi, o non è mai causalmente indispensabile o non è sempre causalmente essenziale alla concretizzazione della lesione patrimoniale individuale[233].

Inoltre, sempre nell'interesse dell'analisi relativa alla tutela penale del patrimonio, nonché della successiva disamina dei crimini oggetto del presente elaborato, è meritevole di menzione il fatto che, se si valuta l'insieme degli elementi costitutivi tipici dei delitti che offendono il patrimonio individuale, si rileva una differenza strutturale tra i reati che comportano un incremento della sfera

---

[227] SCOPINARO, *Internet e reati contro il patrimonio,* cit. 22.

[228] *Ivi*, 22 s.

[229] *Ivi*, 23.

[230] *Ibidem:* «Si realizzano, nel primo caso, fattispecie quali il furto o il danneggiamento e, nel secondo caso, fattispecie quali la truffa o l'estorsione».

[231] *Ibidem*.

[232] *Ivi*, 24.

[233] *Ivi*, 24 s.

patrimoniale del soggetto attivo e un danno a quella del soggetto passivo, e i reati che, invece, consistono esclusivamente nel danneggiamento del patrimonio della vittima. Nel primo caso si realizzano fattispecie tipiche acquisitive, dato che l'agente acquisisce, appunto, un vantaggio patrimoniale effettivo dal compimento del reato e procura, correlativamente, al soggetto passivo un danno; nel secondo caso, al contrario, dalla condotta di danneggiamento deriva solo un nocumento delle cose altrui, e non anche un profitto per il soggetto attivo[234].

Per quel che riguarda più specificatamente la determinazione dei modelli di svolgimento dei fatti informatici offensivi del patrimonio individuale, una distinzione può essere effettuata tra i casi in cui l'agente , per mezzo della condotta digitale, riesce a coartare la volontà del soggetto passivo e i casi in cui il soggetto attivo si serve del sistema operativo per compiere in autonomia la lesione al patrimonio individuale, senza che vi sia la necessità di includere nel processo causale la condotta altrui[235]. Nell'ambito del primo gruppo sarà possibile realizzare fattispecie la cui condotta risulterà contraddistinta dall'utilizzo di uno strumento tecnologico comunicativo, come la *mail* o il *web*, tramite il quale si potrà inviare la minaccia o il raggiro; nel secondo gruppo, invece, è essenziale differenziare i fatti di danneggiamento dai fatti tipici acquisitivi, poiché «mentre nel primo caso l'interazione con il sistema operativo consisterà nel procurare una disfunzione del sistema o una mera perdita di dati, nel secondo caso l'agente sfrutterà le funzioni del sistema operativo per ottenere il vantaggio patrimoniale a cui mira, senza causare alcuna disfunzione»[236].

I riferimenti fin qui proposti relativamente alle peculiarità della condotta digitale assumono rilevanza non solo nell'identificazione dei reati informatici, ma anche nella ridefinizione della tutela patrimoniale nel cyberspazio.

---

[234] Per approfondire sul punto v. SCOPINARO, *Internet e reati contro il patrimonio,* cit., 27: «[…]dal punto di vista dell'offesa patrimoniale la condotta di danneggiamento si distingue dalle fattispecie tipiche acquisitive poiché l'agente non acquisisce alcun vantaggio concreto dal compimento del reato».

[235] A tal proposito è bene precisare già da ora che la truffa *ex* art. 640 c.p., anche se commessa *on-line,* è un tipico esempio di fattispecie a cooperazione artificiosa, diversamente dalla frode informatica *ex* art. 640-*ter* c.p. che rappresenta un modello di aggressione unilaterale; tuttavia, si tratta in entrambi i casi di fattispecie tipiche acquisitive.

[236] *Ivi*, 31 s.

Dunque, per concludere, è opportuno precisare che con il termine "*Financial cybercrime*" si è soliti indicare qualunque reato informatico, solitamente commesso a scopo di profitto, che lede il patrimonio di un individuo ovvero il sistema economico-finanziario nel suo complesso; si tratta di crimini realizzati nella maggior parte dei casi *on-line*, e ciò giustifica l'utilizzo del prefisso *cyber* nella denominazione. Anche se non esiste una puntuale tassonomia dei reati inclusi in questa categoria, la dottrina ricomprende al suo interno la frode informatica, la truffa *on-line* e il *phishing* – quali ipotesi di reato oggetto di successivo approfondimento di questa tesi–, la frode nei sistemi di pagamento, il riciclaggio, l'autoriciclaggio, la ricettazione e il *trading* illegale.

2.2 Il delitto di truffa *on-line ex* art. 640 c.p.: inquadramento normativo.

Il delitto di truffa *on-line* non è espressamente previsto nel Codice penale, bensì rappresenta l'esito di un processo ermeneutico relativo all'art. 640 c.p. che contempla il tradizionale reato di truffa. Si tratta, infatti, di una fattispecie che nasce dall'unione degli elementi costitutivi della suddetta fattispecie di truffa con le peculiarità proprie del cyberspazio, luogo in cui tale delitto si rivela facilmente realizzabile[237]. Dunque, l'incessante evoluzione dei mezzi tecnologici e la continua espansione dell'ambiente digitale hanno comportato la necessità di adattare al nuovo contesto le fattispecie di reato tradizionalmente previste, alla luce delle tipicità informatiche e telematiche. In particolare, la crescente opportunità, e talvolta l'esigenza, di svolgere azioni ordinarie e straordinarie, più o meno complesse, in rete hanno potenzialmente incrementato le possibilità di realizzare condotte fraudolente *on-line*, tra cui la truffa nella dimensione telematica.

Ad ogni modo, senza voler anticipare quanto si approfondirà in seguito, è bene precisare già da ora che le condotte digitali sono caratterizzate da elementi di valore propri e diversi rispetto a quelli riscontrabili nei comportamenti materiali, quindi la suindicata condotta digitale si basa su presupposti e modalità di realizzazione distinti da quelli tipici della condotta tradizionale, in ragione del differente ambiente operativo[238].

---

[237] MALETTA, *Il lato oscuro dell'*e-commerce *e i nuovi reati digitali: dalla truffa online alla frode informatica,* in *Salvis juribus,* 11 giugno 2020.

[238]Sul punto v. SCOPINARO, *Internet e reati contro il patrimonio,* cit., 225 s.

In generale, la tipica condotta truffaldina consiste nell'indurre in errore un soggetto, mediante artifici o raggiri, conseguendo un ingiusto vantaggio, per sé o per qualunque altra persona, e causando contestualmente un danno patrimoniale altrui. La determinazione del danno e del profitto deriva da un atto di disposizione patrimoniale, quale requisito implicito del delitto, posto in essere dal soggetto ingannato conseguentemente all'errore[239].

Il contesto prediletto, seppur non esclusivo, per il compimento del reato di truffa *on-line* è quello del commercio telematico, svolto mediante apposite piattaforme *e-commerce*, su cui si avrà modo di indagare più avanti. In questi casi, poiché si realizzano negozi giuridici informatici, la truffa *on-line* assume la forma del c.d. "reato in contratto" – si parla a tal proposito di truffa contrattuale telematica – che criminalizza la condotta antecedente alla stipula di un contratto.

Infatti, la fattispecie in esame incrimina la condotta fraudolenta, compiuta in rete, di chi con artifici o raggiri induce in errore il soggetto passivo, convincendolo a concludere un contratto non voluto[240]; in altre parole, nella truffa contrattuale, sia tradizionale che *on-line*, il patto stipulato è il risultato di artifici o raggiri, poiché senza di essi il soggetto coinvolto non lo avrebbe concluso, oppure lo avrebbe fatto ma ad altre condizioni.

In tale ambito questa fattispecie è volta, pertanto, a salvaguardare i numerosi acquirenti, c.d. "consumatori digitali", e più precisamente il patrimonio e l'autodeterminazione negoziale degli utenti, da eventuali condotte ingannatorie perpetrate sulle piattaforme telematiche.

2.2.1 Il reato di truffa tradizionale *ex* art. 640 c.p.

Al fine di inquadrare correttamente in termini giuridici il nuovo fenomeno truffaldino perpetrato *on-line* non si può che partire dall'esame della tradizionale figura *criminis* di cui all'art. 640 c.p.

Dunque, poiché il fatto commesso *on-line* non è autonomamente disciplinato, è bene individuare i caratteri propri del classico delitto di truffa,

[239] In argomento v. ANTOLISEI, *Manuale di diritto penale*, cit., 472 e 478.
[240] Sul punto v. MALETTA, *Il lato oscuro dell'*e-commerce, cit.

affinché sia possibile sottolineare, successivamente, le principali analogie e differenze tra i due.

La truffa[241], prevista dall'art. 640[242] del Codice penale, rappresenta l'emblema dei delitti fraudolenti contro il patrimonio: «è la frode per eccellenza».

La parola chiave del delitto in esame è l'"inganno", infatti, come si evince dal testo dell'articolo, è per mezzo di esso che la vittima è indotta a compiere un atto pregiudizievole per il suo patrimonio con profitto dell'agente o di terzi; si tratta, perciò, di un reato caratterizzato dal fatto che il consenso della vittima è ottenuto fraudolentemente[243]. In tal caso il soggetto, mediante artifici o raggiri, determina l'autodanneggiamento della vittima, la quale, dunque, pone in essere un atto che importa, per sé, una diminuzione patrimoniale e, per altri, un ingiusto vantaggio[244].

Sulla base di quanto detto, è possibile affermare che si tratta di un reato a forma vincolata, nonché di una fattispecie di cooperazione artificiosa, in quanto è necessaria la collaborazione di un altro individuo, diverso dall'agente, per la realizzazione del reato, che assume, quindi, la qualificazione di "reato plurioffensivo", poiché lesivo non solo del patrimonio ma anche della libertà morale o di autodeterminazione dell'individuo stesso, oltreché, talvolta, della fiducia individuale[245]. Dunque, l'intento della figura *criminis* in esame è da ravvisarsi sia nella salvaguardia del patrimonio che nella tutela della libertà del consenso nei negozi patrimoniali[246].

---

[241] In argomento v. MARTONE, *Il delitto di truffa nella recente giurisprudenza: la dibattuta questione della c.d. truffa processuale*, in *De Iustitia*, 2017, 4, 150. Si tratta di un reato che è stato acquisito di recente nel sistema penale moderno, e che nel tempo è stato oggetto di numerose pronunce giurisprudenziali che ne hanno ridefinito i confini interpretativi.

[242] L'art. 640, collocato sistematicamente nel Libro II del Codice penale, al Titolo XIII, Capo II, definisce, al comma 1, la truffa nel seguente modo: «Chiunque, con artifici o raggiri, inducendo taluno in errore, 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 […] ».

[243] In argomento v. ANTOLISEI, *Manuale di diritto penale,* cit., 472: proprio la presenza del consenso della vittima, seppur conseguenza dell'inganno, distingue il reato di truffa dal furto e dall' appropriazione indebita, quali reati che presuppongono il disaccordo della vittima.

[244] *Ibidem:* la differenza tra il delitto di truffa e quello di estorsione si ravvisa nel fatto che «nel primo la vittima è indotta fraudolentemente all'atto di disposizione patrimoniale, mentre nel secondo è coartata[…]; nell' uno la volontà è viziata da errore, nell' altro è viziata da violenza o minaccia».

[245] Sul punto v. SCOPINARO, *Internet e reati contro il patrimonio,* cit. 23 s.

[246] V. ANTOLISEI, *Manuale di diritto penale,* cit., 472; della stessa convinzione LUCARELLI, *Le truffe,* in CENDON (a cura di), *La prova e il quantum nel risarcimento del danno non patrimoniale,* Torino, 2008, 1993 secondo cui «[…]il reato di truffa avrebbe, cioè, natura plurioffensiva, ledendo al contempo sia il patrimonio, sia la libertà negoziale»; tuttavia, una parte minoritaria della dottrina sembra essere di diversa opinione, v. RONCO, ROMANO, *Codice penale commentato*, 4ª ed., Torino,

Per quel che concerne il bene giuridico patrimoniale si rinvia alle considerazioni fatte precedentemente (v. *supra* §2.1), mentre con riguardo alla libertà di autodeterminazione è opportuno precisare che il pregiudizio all'autodeterminazione – a cui segue la disposizione patrimoniale – consiste nell'impedire alla vittima di decidere consapevolmente e razionalmente, in ragione dell'induzione in errore operata mediante l'impiego di artifici e raggiri, i quali influenzano la libera facoltà di scelta del soggetto, inducendolo ad autodanneggiarsi; infatti, il consenso è un elemento necessario per la sussistenza del reato. Il principio di autodeterminazione, seppur non espressamente richiamato dalla Costituzione, è da considerarsi incluso tra quelli – ad esempio artt. 2 e 3 Cost. – che riconoscono la centralità dell'individuo e della sua personalità.

È indubbio, peraltro, che nel *web* l'offesa al patrimonio e soprattutto alla libertà di autodeterminazione si realizza in modo più subdolo, attraverso il compimento della truffa telematica, di cui tratterà in dettaglio più avanti.

La truffa rappresenta una delle figure criminose più complesse, poiché ricomprende, in concreto, numerosi fatti che mostrano notevoli differenze tra loro.

2012, 3263, che richiama in nota PEDRAZZI, *Inganno ed errore nei delitti contro il patrimonio*, Milano, 1955, 34, e ZANNOTTI, *La truffa*, Milano, 1993, 14: «Nondimeno, talune voci minoritarie propendono per la natura monoffensiva del delitto in esame, che sarebbe rivolto a tutelare il solo patrimonio, laddove la lesione alla libertà del consenso integrerebbe unicamente la specifica modalità di aggressione tipizzata dal legislatore, senza assurgere al rango di bene giuridico tutelato»; inoltre, in argomento v. MARRA, *Truffa*, in FIORE (diretto da), *I reati contro il patrimonio*, Torino, 2010, 482 e 484 s: «a differenza di quanto avviene in relazione ad altre fattispecie incriminatrici contenute nel Titolo XIII, dove la componente patrimoniale è destinata a convivere con interessi di altra natura già a livello di selezione del tipo (rapina, estorsione, usura, ecc.), nella truffa l'esclusività della prospettiva patrimoniale emerge anche su questo piano e raccoglie un diffuso consenso. Tale sostanziale uniformità di vedute, non intaccata dalla presenza di una pluralità di voci propense a ricostruire l'oggettività giuridica in termini di plurima offensività nei confronti del patrimonio e della buona fede dell'ingannato, non può tuttavia far perdere di vista l'esistenza di ''sfumature'' che, oltre a consentire una migliore comprensione della dinamica interpretativa della fattispecie in commento, molto sembrano poter dire in ordine alla sostanza politico-criminale delle diverse letture della fattispecie incriminatrice.[…] Il bene giuridico va dunque identificato nel patrimonio (qui salvaguardato) riguardo alla libertà di disporne al riparo da capziose intromissioni altrui […].[…]al centro di ogni riflessione avente ad oggetto la definizione del bene giuridico tutelato dal delitto di truffa, la buona fede della vittima e la sua libertà di scelta entrano a comporre il substrato dell'oggetto di tutela e, in ragione di ciò, concorrono in misura decisiva a specificare la dimensione offensiva del fatto[…].[…]l'ampliamento dell'oggettività giuridica al c.d. ''diritto alla verità'' non deve essere inteso come un ampliamento personalistico del bene giuridico tutelato. La buona fede della vittima e la sua libertà di scelta sono qui intese come presupposti necessari del potere di decidere dei destini della propria sfera patrimoniale. La loro lesione non deve pertanto considerarsi offesa ad un bene della personalità ma solo come violazione dell'autonomia dispositiva della vittima[…]».

Tuttavia, dalla definizione legislativa si deduce che la fattispecie oggettiva della truffa, in linea generale, risulta costituita dai seguenti elementi: il primo è il particolare comportamento del reo, indicato con la formula "artifizi e raggiri"; il secondo riguarda la causazione dell'errore dal quale deve generarsi la disposizione patrimoniale; l'ultimo si riferisce al danno patrimoniale, determinato dall'inganno, e al relativo profitto per il soggetto attivo o per altri[247].

Innanzitutto, in merito al primo elemento, relativo al comportamento dell'agente[248], è opportuno chiarire il significato dell'espressione "artifizi o raggiri": l'"artifizio" consiste in un «camuffamento della realtà effettuato sia simulando ciò che non esiste[…], sia dissimulando, vale a dire, nascondendo, ciò che esiste[…]»[249], e agisce sulla realtà esterna, elaborando una fittizia apparenza materiale; il raggiro, invece, «è un avvolgimento ingegnoso di parole destinate a convincere: più precisamente, una menzogna corredata da ragionamenti idonei a farla scambiare per verità»[250], e interviene direttamente sulla psiche del soggetto raggirato. Ad ogni modo, la giurisprudenza rileva che, qualunque sia il senso attribuito agli artifici e raggiri, la loro attitudine a trarre in inganno un soggetto deve essere valutata con riferimento alla concreta situazione verificatasi[251].

L'opinione secondo cui la formula legislativa considerata reclami una spiccata furbizia e un'ingegnosa strategia nel realizzare l'inganno, con il tempo, nella prassi, si è sempre più indebolita, fino a svanire; infatti, ad oggi, sia la dottrina preminente che la gran parte della giurisprudenza concordano nel senso di ritenere che anche la mera menzogna sia sufficiente ad integrare il reato di truffa[252].

Il silenzio e la reticenza, rappresentando comportamenti neutri, hanno sollevato non pochi dubbi circa loro idoneità ad integrare il delitto in esame.

---

[247] In argomento ANTOLISEI, *Manuale di diritto penale,* cit., 473.

[248] Il soggetto attivo può essere "chiunque", si tratta infatti di un reato comune.

[249] Cfr. ANTOLISEI, *Manuale di diritto penale,* cit., 474.

[250] *Ibidem*.

[251] Sul punto v. MARTONE, *Il delitto di truffa,* cit., 153; v. Trib. di Milano 19 maggio 2006, in *Red. Giuffrè*, 2007, richiamata anche in nota da ANTOLISEI, *Manuale di diritto penale,* cit., 475: «L'adeguatezza degli artifici e raggiri va valutata non in relazione ad una generica idoneità dei mezzi utilizzati a trarre in inganno, ma con riferimento diretto alla particolare situazione in cui è avvenuto il fatto e alle modalità esecutive dello stesso».

[252] Sul punto v. Cass. pen., 1° dicembre 2010, n. 24718, in *C.E.D Cass*., rv. 248662, secondo cui «integra l'elemento costitutivo del reato di truffa anche la sola menzogna, costituendo una tipica forma di raggiro»: menzionata anche in nota da ANTOLISEI, *Manuale di diritto penale,* cit., 475.

Tuttavia, il quesito si è risolto in senso affermativo laddove vi sia in capo al soggetto attivo uno specifico obbligo giuridico di comunicazione ovvero laddove venga offeso il principio di buona fede[253].

Gli artifici e i raggiri, quindi, rappresentano le precise modalità di realizzazione della condotta, rendendo la truffa un reato a forma vincolata[254].

Il secondo elemento attiene all'errore; infatti, il comportamento del soggetto attivo deve indurre in errore il soggetto passivo: in altre parole, gli artifici o i raggiri posti in essere dall'agente devono essere fonte di un inganno che, a sua volta, deve originare un danno patrimoniale. Inoltre, non è più richiesta la particolare attitudine o idoneità ingannatoria del mezzo usato, poiché, attualmente, si ritiene bastevole che gli artifici o raggiri abbiano in concreto provocato il suddetto inganno, risultando ininfluente il fatto che l'ignoranza o la superficialità del soggetto passivo possano aver facilitato l'errore[255]. Tuttavia, per integrare il reato di cui all'art. 640 c.p. non è necessario dover trarre in inganno un soggetto, poiché può risultare sufficiente anche l'aver approfittato di un errore già esistente. È bene puntualizzare, però, che il soggetto attivo deve aver posto in essere, seppur minimamente, un'attività volta a consolidare il suddetto errore.

Ad ogni modo, non si può non precisare che tale errore non può di per sé causare il danno patrimoniale che è necessario per l'esistenza del reato in esame, e, pertanto, deve essere disposto dal soggetto ingannato un apposito atto volto a produrre detto nocumento, delineandosi così il requisito implicito della truffa,

[253] Sul punto v. MARTONE, *Il delitto di truffa,* cit., 152.

[254] V. MARZULLO, *Truffa informatica*, in *Arch. Pen.*, 2017, 3, 5.

[255] In argomento v. Cass. pen., 3 luglio 2009, n. 34059, in *C.E.D. Cass.*, rv. 244948, richiamata anche in nota da ANTOLISEI, *Manuale di diritto penale,* cit., 477.

ravvisabile nella c.d. "disposizione patrimoniale"[256], la quale può avere anche carattere omissivo[257].

Inoltre, l'inganno deve rivolgersi ad un soggetto determinato, anche diverso da quello che subisce il danno patrimoniale[258]: non è dunque necessaria l'identità tra l'individuo indotto in errore e quello che ne patisce le conseguenze negative, purché esista un rapporto causale tra l'induzione in errore e gli elementi di profitto e danno[259].

Il terzo elemento riguarda il danno patrimoniale ed il contestuale ingiusto profitto altrui, quali conseguenze del suindicato atto di disposizione: si parla, dunque, di duplice evento[260].

---

[256]Cfr. Cass. pen., Sez. Un., 29 settembre 2011, n. 155, in *C.E.D Cass.*, rv.251499: relativamente alla definizione di atto di disposizione patrimoniale le Sezioni Unite hanno indicato che «ai fini della configurabilità del delitto di truffa, l'atto di disposizione patrimoniale, quale elemento costitutivo implicito della fattispecie incriminatrice, consiste in un atto volontario, causativo di un ingiusto profitto altrui a proprio danno e determinato dall' errore indotto da una condotta artificiosa; ne consegue che lo stesso non deve necessariamente qualificarsi in termini di atto negoziale, ovvero di atto giuridico in senso stretto, ma può essere integrato anche da un permesso o assenso, da una mera tolleranza o da una *traditio*, da un atto materiale o d un fatto omissivo, dovendosi ritenere sufficiente la sua idoneità a produrre un danno»; v. ANTOLISEI, *Manuale di diritto penale*, cit., 478 s., secondo cui al di là del già citato consenso, un ulteriore elemento di distinzione tipico della truffa rispetto ai reati di furto e appropriazione indebita è rappresentato proprio dalla disposizione patrimoniale, poiché è lo stesso soggetto ingannato che, a seguito dell' errore, cagiona contestualmente il danno patrimoniale e il profitto altrui; è bene aggiungere, altresì, che «l' atto dispositivo può avere per oggetto qualsiasi elemento del patrimonio, e, perciò, non solo i beni mobili […] come nel furto e nell' appropriazione indebita, ma anche i beni immobili e i diritti di qualsiasi specie. Può avere per oggetto pure servizi personali e cioè prestazioni di opera, di ospitalità, di beneficienza[…]».

[257] Sul punto v. Cass. pen., 2 gennaio 2008, n. 2808, in *C.E.D. Cass.*, rv 242649, come indicato da ANTOLISEI, *Manuale di diritto penale*, cit., 479: « […] il danno della vittima può realizzarsi non soltanto per effetto di una condotta commissiva, bensì anche per effetto di un suo comportamento omissivo, nel senso che essa, indotta in errore, ometta di compiere quelle attività intese a fare acquisire al proprio patrimonio una concreta utilità economica, alla quale ha diritto e che rimane invece acquisita al patrimonio altrui[…]».

[258] A tal proposito, è bene precisare che il soggetto vittima dell'inganno deve trovarsi in una situazione giuridica idonea a poter compiere l'atto di disposizione patrimoniale: in argomento v. ANTOLISEI, *Manuale di diritto penale*, cit., 480 ss., anche con riferimento al tema della truffa processuale. L'A. segnala inoltre che, ad oggi, sia la dottrina che la giurisprudenza sembrano concordare sul fatto che sia configurabile il reato di truffa in tutti i casi in cui il soggetto ingannato sia stato truffato mentre egli stesso cercava di realizzare un fine illecito, poiché le ragioni fondanti di tale delitto non vengono meno quando la vittima opera con un fine illegale, trattandosi in tal caso di "truffa in atti illeciti".

[259] Sul punto v. Trib. Frosinone, 12 Settembre 2020, n. 795, in *Red. Giuffrè*, 2020 secondo cui per l'integrazione del reato di truffa non è essenziale l'identità tra l'ingannato e colui che ha subito il danno patrimoniale, «purché, anche in assenza di contatti diretti fra il truffatore e il truffato, sussista un nesso di causalità tra l'induzione in errore, il profitto ed il danno»; in tal senso v. anche Corte App. Lecce, 7 settembre 2020, n. 602, in *Red. Giuffrè*, 2020; v. anche Cass. pen., Sez II, 21 febbraio 2008, n. 10085, in *www.exeo.it.*

[260] V. MARZULLO, *Truffa informatica*, cit., 5.

Tale danno consiste in una *deminutio patrimonii*, riferendosi a tutte le cose oggetto del patrimonio, tra cui anche quelle che, in base alla condivisa nozione patrimoniale di cui si è detto, hanno un mero valore di affezione.

Secondo quanto sostenuto dall'opinione prevalente, il nocumento si verificherebbe non solo in caso di perdita di un bene, ma anche in ragione del mancato ottenimento di un'utilità patrimoniale che la vittima avrebbe voluto acquisire[261].

Il summenzionato pregiudizio deve essere valutato con criteri oggettivi, tenendo conto, quindi, dell'opinione della collettività e non del singolo che lo subisce, ma è bene avere presenti anche le peculiarità del caso concreto.

Il profitto, corrispondente al nocumento, è qualificato come "ingiusto", ed è attribuibile all'agente o a terzi; inoltre, anch'esso ha natura patrimoniale, e quindi non necessariamente economica.

Il reato di truffa è un reato istantaneo e di evento, la cui consumazione si ha nel momento in cui si realizza l'ingiusto vantaggio con l'altrui danno[262]. In altre parole, il conseguimento del profitto con l'altrui *deminutio patrimonii* indica il momento consumativo del delitto di truffa[263], ravvisandosi così la possibilità di configurare il tentativo del reato in esame ogniqualvolta alla condotta truffaldina non consegua siffatta realizzazione. A tal proposito è opportuno rilevare che «per accertare l'idoneità del mezzo – requisito essenziale del tentativo – vanno tenute presenti tutte le circostanze del caso concreto che, al momento dell'azione, potevano essere conosciute»[264].

Ad ogni modo, per quel che concerne, più precisamente, l'articolata questione relativa al momento consumativo e all'individuazione del *locus commissi delicti* della truffa commessa *on-line,* si rinvia ad una fase successiva.

---

[261] In argomento v. MARTONE, *Il delitto di truffa,* cit., 153.

[262] Sul punto v. *ibidem*: l'Autore inoltre afferma che «il *locus commissi delicti* del delitto di truffa si identifica nel luogo dove l'agente consegue il profitto a seguito dell'effettiva *deminutio patrimonii* della vittima». Si tratta, dunque, di un reato a doppio evento consumativo.

[263] V. ANTOLISEI, *Manuale di diritto penale,* cit., 484 s.; dunque, si deve tener conto del momento in cui si realizzano l'effettivo danno patrimoniale per la vittima e il profitto per l'agente.

[264] Cfr. ANTOLISEI, *Manuale di diritto penale,* cit., 486.

L'elemento soggettivo richiesto dal delitto in esame è il dolo generico[265], poiché il soggetto attivo deve volere la sua condotta, il conseguente inganno del soggetto passivo, la successiva disposizione patrimoniale, nonché la realizzazione del danno ed il contestuale conseguimento del profitto. Inoltre, la volontà dell'agente deve essere associata alla consapevolezza del carattere truffaldino del mezzo impiegato, del danno al patrimonio della vittima e dell'ingiustizia del vantaggio patrimoniale perseguito[266].

L'ipotesi aggravata del reato considerato è configurabile ogniqualvolta ricorra una delle seguenti circostanze: «se il fatto è commesso a danno dello Stato o di un altro ente pubblico o col pretesto di far esonerare taluno dal servizio militare; se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dover eseguire un ordine delle Autorità; se il fatto è commesso in presenza della circostanza di cui all'art. 61, numero 5»[267].

In virtù della possibilità, di cui si dirà in seguito, di configurare l'ultima circostanza aggravante, di cui all'art. 61, comma 1, n. 2-*bis*, nel caso di truffa commessa *on-line*, sembra opportuno precisare che la suddetta circostanza speciale è stata introdotta dall'art. 3 comma 28 della legge 94/2009, e rievoca l'aggravante generica della c.d. "minorata difesa" *ex* art. 61 n. 5 c.p., al fine di sanzionare più severamente le condotte truffaldine poste in essere in danno dei soggetti che, per circostanze di tempo, di luogo, di persona o di età, risultano più deboli[268].

---

[265] Sul punto v. Corte App. Lecce, 9 settembre 2020, n. 506, in *Red. Giuffrè*, 2020: «in merito all'imputazione per il delitto di truffa, […] con riferimento all' elemento soggettivo va rilevato che, ai fini della sussistenza del reato, è sufficiente il dolo generico, sicché non si richiede che l'agente sia animato da alcun fine di maltrattare la vittima, bastando la coscienza e volontà di sottoporre la stessa alla propria condotta abitualmente offensiva»; in merito v. anche Trib. Nola, 21 maggio 2020, n. 780, in *Red. Giuffrè*, 2020.

[266]In argomento v. Cass. pen., sez. V, 9 settembre 2020, n. 30726, in *C.E.D. Cass.*, rv. 279908-01: «In tema di truffa, la prova dell'elemento soggettivo, costituito dal dolo generico, diretto o indiretto, può desumersi dalle concrete circostanze e dalle modalità esecutive dell' azione criminosa, attraverso le quali, con processo logico-deduttivo, è possibile risalire alla sfera intellettiva e volitiva del soggetto, in modo da evidenziare la cosciente volontà e rappresentazione degli elementi oggettivi del reato, quali l' inganno, il profitto ed il danno, anche se preveduti come conseguenze possibili della propria condotta, di cui si sia assunto il rischio di verificazione».

[267] Cfr. Art. 640, comma 2, c.p.

[268] Cfr. ANTOLISEI, *Manuale di diritto penale*, cit., 491: «È stato evidenziato che la novella ha, in buona sostanza, trasformato una circostanza aggravante comune in una circostanza speciale con l'effetto di amplificare la pena commutabile; per la forma aggravata, diversamente da quella semplice, è prevista la reclusione da uno a cinque anni e la multa da 309 a 1549 euro. Inoltre, come disposto dal dettato legislativo dell'art. 640 c.p. «il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal capoverso precedente o la circostanza aggravante prevista dall'articolo 61, primo comma, numero 7».

La disamina sin qui svolta, relativa alla figura della truffa tradizionale, semplice e aggravata, è finalizzata a definire i tratti essenziali della truffa commessa *on-line*, su cui è ora possibile concentrarsi.

2.2.2 Le caratteristiche del reato di truffa *on-line*

Come anticipato, il delitto di truffa può realizzarsi anche mediante l'utilizzo di strumenti tecnologici o per mezzo della rete, infatti nel tempo l'ambiente digitale ha rivelato di essere lo scenario prescelto per la messa a punto dei sistemi truffaldini; tuttavia, si tratta di ipotesi di manifestazione del reato non autonomamente disciplinate dal Codice penale, ragion per cui devono essere ricondotte alla formula legislativa relativa al reato di truffa tradizionale di cui all'art. 640 c.p., rispetto al quale si rileva un'esigenza di adattamento e riconsiderazione sulla base delle innovazioni tecnologiche affermatesi.

A seguito della disamina proposta in merito al reato di truffa tradizionale, e con riguardo alle peculiarità proprie del cyberspazio, è possibile individuare gli elementi caratterizzanti del delitto di truffa commesso *on-line*, sottolineando altresì analogie e differenze con la comune figura *criminis.* Si propone, dunque, un'interpretazione del fenomeno truffaldino alla luce della realtà cibernetica in cui si realizza il fatto.

Innanzitutto, è bene rievocare le caratteristiche inerenti al *cyberspace*, quale contesto di commissione del reato di truffa *on-line*: smaterializzazione, anonimato, atemporalità, aterritorialità e rapidità delle comunicazioni contraddistinguono, infatti, la nuova dimensione, agevolando e variando le modalità di compimento di determinate figure di reato, tra le quali quella in esame.

È utile premettere che sussiste una differenza di valore tra le condotte poste in essere nella realtà materiale e quelle realizzate nell'ambiente digitale, e che tale difformità non si ravvisa solo nella possibilità di individuare nel fatto gli elementi prescritti dalle fattispecie tipiche esistenti relative a fatti materiali, ma si riflette anche sul contenuto lesivo degli elementi essenziali del reato, esigendo una rivalutazione della capacità offensiva e degli interessi coinvolti[269].

[269] In argomento v. SCOPINARO, *Internet e reati contro il patrimonio*, cit., 225.

La truffa realizzata a mezzo Intenet, al pari di quella comune, è una fattispecie plurioffensiva, infatti, rispetto al delitto tradizionale restano invariati i beni giuridici penalmente rilevanti, quali il patrimonio e l'autodeterminazione degli utenti. Tuttavia, il compimento delle condotte ingannevoli, offensive dei suddetti beni, risulta in tale contesto notevolmente agevolato[270], in ragione dell'assenza di contatto materiale fra l'utente e l'agente, e della copertura dell'anonimato di cui si avvale, a determinate condizioni, quest'ultimo, nonché dalla rapidità tipica delle azioni stesse perpetrate sul *web*.

Alla luce delle tipicità della rete, può affermarsi che, in tal caso, i comportamenti posti in essere risultano più pericolosi ed ingannevoli, e che la lesione ai predetti beni giuridici si manifesta in modo più incisivo e subdolo, poiché l'agente sfrutta le suddette facilitazioni per fini criminosi, scegliendo, talvolta volutamente, di compiere tali azioni delittuose in un contesto che predispone condizioni più favorevoli rispetto all'ambiente materiale, prediligendolo, dunque, per la realizzazione del reato di truffa[271]. Si ravvisa, perciò, un diverso disvalore della condotta, il quale si accentua e aggrava se il comportamento antigiuridico è perpetrato in rete.

Da quanto sin qui detto si evince, altresì, che il cybercriminale assume una posizione di vantaggio nei confronti della vittima, poiché egli è consapevole della maggiore vulnerabilità del soggetto passivo nel contesto telematico, e sfrutta le peculiarità ad esso afferenti – prima fra tutte la suindicata mancanza di contatto materiale fra utente e agente[272] – per ottenere un ingiusto profitto.

Le caratteristiche del "non luogo" informatico sono state valorizzate dalla giurisprudenza di legittimità al fine di poter integrare la circostanza aggravante speciale contemplata dall'art. 640, comma 2, n. 2-*bis* che richiama espressamente la circostanza aggravante generica *ex* art. 61, n. 5, c.p, inerente alla c.d. "minorata

[270] Sull'incremento delle condotte fraudolente offensive del patrimonio e dell'autodeterminazione degli utenti del *web* v. PECORELLA, DOVA, *Profili penali delle truffe on-line,* in *Arch. pen.*, 2013, 3, 799 s.

[271] Si osserva che la comune condotta fraudolenta incontra le tipicità del *cyberspace* e viene da esse facilitata.

[272] V. SCOPINARO, *Internet e reati contro il patrimonio,* cit., 166.

difesa"[273]. Secondo quanto sostenuto dalla Suprema Corte di Cassazione[274], infatti, nell'ambito delle truffe *on-line* sarebbe configurabile l'aggravante di cui all'art. 640 comma 2, n. 2-*bis*, relativa alla minorata difesa, in virtù della posizione di maggior favore dell'agente rispetto alla vittima[275].

Le condotte truffaldine, in ragione delle particolari ed innumerevoli modalità di realizzazione dovute alle tipicità del *web*, presentano una più intensa potenzialità offensiva nei confronti dei beni giuridici meritevoli di protezione, aumentando così il proprio disvalore penale. I cybercriminali riescono a ricavare un ingiusto profitto con altrui danno patrimoniale ponendo in essere una condotta meno impegnativa, ovverosia uno sforzo minore per indurre in errore il soggetto passivo, poiché tra i due soggetti si interpone il mezzo telematico che facilita l'agente, e, a differenza della condotta tradizionalmente intesa, l'offesa ai detti beni giuridici risulta essere più grave, in virtù di un più subdolo inganno.

Nell'ambiente materiale, al contrario, l'agente ha inferiori *chance* di ingannare la vittima, poiché quest'ultima, alla luce della sussistenza di un contatto materiale con l'impostore, è messa nella condizione di poter riconoscere più agevolmente l'inganno.

La truffa *on-line*, come quella tradizionale, è una fattispecie di profitto la cui condotta si fonda sulla cooperazione artificiosa fra il soggetto attivo ed un altro soggetto definito "ingannato", il quale, come evidenziato nell'ambito dell'analisi del reato di truffa comune, non deve necessariamente identificarsi con il soggetto che subisce il pregiudizio patrimoniale[276]. Tuttavia, nella truffa commessa *on-line*, in conseguenza della dematerializzazione e degli automatismi, la rilevanza dell'elemento di cooperazione artificiosa sembrerebbe subire un ridimensionamento, poiché la partecipazione dell'utente ingannato alla

---

[273] Sul punto v. MINICUCCI, *Le frodi informatiche*, in CADOPPI, CANESTRARI, MANNA, PAPA (diretto da), *Cybercrime*, Torino, 2019, 840 s.

[274] Cfr. Cass., pen., Sez. II, 29 settembre 2016, n. 43705, in *www.dirittopenale.it*, in cui si osserva che: «la distanza tra il luogo di commissione del reato, ove l'agente si trova, ed il luogo ove si trova l'acquirente del prodotto on line - che ne abbia pagato anticipatamente il prezzo, secondo quella che rappresenta la prassi di simili transazioni - è l'elemento che consente all'autore della truffa di porsi in una posizione di maggior favore rispetto alla vittima, di schermare la sua identità, di fuggire comodamente, di non sottoporre il prodotto venduto ad alcun efficace controllo preventivo da parte dell'acquirente; tutti vantaggi che non potrebbe sfruttare a suo favore, con altrettanta comodità, se la vendita avvenisse *de visu*»; v. anche Cass. pen., Sez. VI, 10 aprile 2017, n. 17937.

[275] V. MALETTA, *Il lato oscuro dell'*e-commerce, cit.

[276] Cfr. SCOPINARO, *Internet e reati contro il patrimonio*, cit., 163.

realizzazione del fatto criminoso sarebbe nettamente ridotta, dal momento che la condotta truffaldina non potrebbe più associarsi alla materialità, divenendo percepibile solo per via telematica, in virtù del difetto di contatto diretto tra le parti. In altre parole, la collaborazione del soggetto passivo sembrerebbe avere, ai fini della commissione del delitto in esame, un peso minore rispetto a quello assunto nel reato comune, poiché la smaterializzazione avvantaggerebbe già da sé l'agente. Ad ogni modo non si potrebbe sostenere l'assenza del suddetto elemento, poiché considerato requisito essenziale e distintivo della truffa, anche se commessa *on-line*; dunque, si deve ritenere che, seppur con una minima rilevanza, la presenza della cooperazione artificiosa sia necessaria, poiché a seguito dell'induzione in errore, il soggetto passivo deve sempre compiere un atto di disposizione patrimoniale causativo del danno con profitto altrui[277].

L'ulteriore elemento della fattispecie tradizionale che subisce una variazione è quello dell'induzione in errore, il cui esame è strettamente connesso al suindicato elemento della cooperazione artificiosa, poiché solo spiegando il mutamento dell'uno è possibile cogliere il ridimensionamento dell'altro. La rete facilita l'azione ingannatoria dell'agente nei confronti di un soggetto passivo che ha ridotte possibilità di rendersi conto dell'inganno, poiché tale "filtro" digitale non consente di percepire la reale prospettazione fatta dall'ingannatore.

Dunque, il contesto digitale, in ragione degli effetti intersoggettivi che provoca, da un lato consente una più semplice predisposizione dell'inganno tipico del reato, e dall'altro rende più complicato il riconoscimento della condotta truffaldina per il soggetto passivo.

Inoltre, a proposito dell'elemento soggettivo, nella maggior parte dei casi di truffa *online* si registra un'elevata difficoltà di accertamento della responsabilità penale che spesso si conclude con l'archiviazione. Si rilevano altresì numerose complicazioni durante la fase investigativa, finalizzata all'individuazione del

[277] *Ivi*, 163: «[…]in questi casi l'interazione con il sistema è funzionalizzata da parte dell'agente alla realizzazione di una coartazione a carico del soggetto che subisce la condotta alla quale segue il compimento da parte di tale soggetto di un atto di disposizione patrimoniale, causa del successivo verificarsi di un evento di profitto a favore dell'agente e di danno a carico del soggetto passivo».

colpevole, soprattutto in ragione dell'impiego di tecniche che assicurano l'anonimato in rete[278].

L'assenza di contatto tra le parti provoca un'elevazione dello *standard* di fiducia e affidamento al soggetto attivo da parte del soggetto passivo, poiché a quest'ultimo non è lasciata altra scelta se non quella di fidarsi dell'agente[279].

Dunque, l'esigua rilevanza della cooperazione artificiosa della vittima e la notevole facilità di induzione in errore della stessa dovute alla smaterializzazione, nonché il maggior disvalore della condotta a cui consegue una più grave offesa ai beni giuridici coinvolti rappresentano le principali differenze tra il reato di truffa comune e quello *onlin*e.

Assunto che, in generale, anche nella truffa commessa a mezzo internet la consumazione del reato debba avvenire "nel momento in cui si verifica l'effettivo conseguimento del bene da parte dell'agente e la definitiva perdita dello stesso da parte del raggirato"[280], si rinvia ad una fase successiva l'analisi del tema, nonché delle relative questioni sulla determinazione del *locus commissi delicti* e del giudice territorialmente competente.

Il fenomeno truffaldino commesso *on-line* è soggetto ad una continua evoluzione, di pari passo con il contesto digitale in cui si realizza, provocando talvolta difficoltà applicative della fattispecie di cui all'art. 640 c.p. che necessiterebbe, dunque, di una ridefinizione alla luce del progresso tecnologico e delle eventuali nuove esigenze di maggior tutela. Tuttavia, a causa di tale inadeguatezza non di rado si rischia di lasciare impuniti gli autori di numerose truffe telematiche[281].

Dunque, sarebbe auspicabile per il futuro una previsione legislativa *ad hoc* capace di fronteggiare autonomamente la condotta truffaldina commessa nel cyberspazio, i cui tratti essenziali possono essere delineati sulla base della disamina dei casi concretamente realizzatisi.

---

[278] Sul punto v. PECORELLA, DOVA, *Profili penali delle truffe* on-line, cit., 799.

[279] In argomento v. CIPOLLA, E-commerce *e truffa*, in *Giur. merito*, 2013, 12, 2630.

[280] Cfr. PECORELLA, *Truffe* on-line*: momento consumativo e competenza territoriale*, in *Dir. pen. cont*., 10 maggio 2012.

[281] In argomento v. CIPOLLA, E-commerce *e truffa*, cit., 2640.

2.2.3 *E-commerce* ed *on-line criminal markets*: il reato di truffa a danno dei consumatori digitali.

Lo sviluppo tecnologico ha favorito ed incentivato la nascita di apposite piattaforme digitali di *e-commerce,* ovverosia piattaforme specializzate ideate per facilitare gli scambi commerciali tra individui[282], ampliando, così, le prospettive economiche di ciascuno di essi: è questo il contesto prediletto per la commissione di truffe *on-line.*

Il commercio *on-line* può svolgersi interamente nel *cyberspace,* poiché la rete si interpone tra il venditore e l'acquirente[283], annullando così qualunque forma di contatto tra le parti e consentendo a chiunque, in qualunque tempo ed ovunque ubicato, di realizzare agevolmente e celermente operazioni di scambio di beni o servizi, talvolta anche in forma anonima, in virtù della smaterializzazione, atemporalità, aterritorialità, rapidità e anonimato, quali caratteristiche tipiche del contesto cibernetico in cui si realizzano.

Nella moderna società dell'informazione *l'e-commerce* è diventato uno strumento fondamentale per le imprese nazionali e internazionali, trattandosi di una modalità di compravendita sempre più comune e sempre più sfruttata da imprenditori e consumatori per l'offerta e l'acquisto di beni o servizi. "Semplificazione" è il termine che meglio definisce il commercio elettronico[284],

---

[282] Tra i più grandi siti di *e-commerce* si ravvisano *ebay*, *Amazon*, Zalando ecc.

[283] CIPOLLA, E-commerce *e truffa*, cit., 2624 s.

[284]Cfr. PATI, E-commerce*, che cos'è e come funziona: regole 2020*, in *www.agendadigitale.eu*, 5 giugno 2020: una prima definizione di "commercio elettronico" è stata fornita dalla comunicazione della Commissione europea n. 157 del 1997, secondo cui «lo svolgimento di attività commerciali e di transazioni per via elettronica e comprende attività quali: la commercializzazione di beni o servizi per via elettronica; la distribuzione on-line di contenuti digitali; l'effettuazione per via elettronica di operazioni finanziarie e di borsa; gli appalti pubblici per via elettronica ed altre procedure di tipo transattivo delle pubbliche amministrazioni». La suindicata definizione sottolinea che il commercio elettronico è solito riferirsi a numerose attività, e che esso può essere "diretto" se la conclusione e l'esecuzione del contratto si realizzano interamente *on-line* – poiché l' utente ottiene digitalmente i beni immateriali – , o "indiretto" se l' esecuzione del contratto avviene tradizionalmente e quindi per mezzo della consegna dell'oggetto materiale; per completezza è bene puntualizzare, inoltre, che la Comunicazione della Commissione europea n. 157 del 1997 è stata attuata dalla Direttiva 2000/31/CE, anche detta "Direttiva sul commercio elettronico", la quale ha sostituito il concetto di "commercio elettronico" con quello più generale di "servizi della società dell'informazione", con l'obiettivo, seppur non ancora raggiunto, di definire un quadro giuridico uniforme in materia. In Italia, la suindicata Direttiva è stata attuata con il D.lgs. 70/2003, al fine di incentivare la libera circolazione dei servizi della società dell'informazione, fra i quali il commercio elettronico, il quale «trova la sua disciplina nel contratto telematico che si conclude a distanza tramite due canali che viaggiano su internet: la posta elettronica e il *World Wide Web*. Ai contratti telematici la dottrina e la giurisprudenza applicano la disciplina

poiché esso consente, tra gli altri, di concludere negozi giuridici utilizzando strumenti telematici, e più precisamente accedendo alle apposite piattaforme digitali situate sul *web* e condividendo documenti informatici, senza la necessaria simultanea presenza delle parti in uno stesso luogo fisico.

Il diffuso utilizzo delle piattaforme di *e-commerce* ha incrementato il rischio di commissione di condotte frodatorie a mezzo *web*, tra le quali la più comune è la truffa, che, in tale ambito, assume la particolare forma della truffa contrattuale, poiché tale fenomeno criminoso si basa su negozi giuridici conclusi per via telematica: dunque, nell'ambito del commercio elettronico le truffe *on-line* rappresentano la versione moderna delle truffe contrattuali[285].

A tal proposito è bene precisare che «integra gli estremi della truffa contrattuale la condotta di chi ponga in essere artifizi o raggiri consistente nel tacere o nel dissimulare fatti o circostanze tali che, ove conosciuti, avrebbero indotto l'altro contraente ad astenersi dal concludere il contratto»[286]. Inoltre, questa forma di truffa può realizzarsi non solo nella fase di conclusione del contratto, ma anche in quella di esecuzione dello stesso, laddove una delle due parti inganni l'altra conseguendo un ingiusto profitto con altrui danno; quindi, sulla base di quanto sostenuto dalla giurisprudenza, nella truffa contrattuale gli artifici o raggiri si ritengono rilevanti anche quando incidono sull'esecuzione del contratto[287].

In altre parole, questo tipo di truffa si concretizza quando l'agente inganna il soggetto passivo inducendolo a concludere un negozio giuridico al fine di conseguire un profitto per sé o per altri con altrui nocumento.

Dunque, la condotta truffaldina nel contesto digitale può realizzarsi per mezzo di una mera finzione, oppure nell'ambito di un rapporto contrattuale se si considera il più circoscritto ambito dei siti *e-commerce,* ed è per tale ragione che in quest'ultimo caso si è soliti parlare di truffa contrattuale telematica.

---

dei contratti in generale contenuta nel Codice civile […]. Oltre alla disciplina dei contratti in generale, nei confronti deli operatori professionali e del consumatore si applica la normativa italiana specifica sul commercio elettronico, emanata con il D.lgs. 70/2003. Se vi è un consumatore si applicano anche le norme predisposte per la sua tutela[…]». A tale ultimo proposito, il Codice del consumo prevede specifiche disposizioni per la tutela del consumatore.

[285] Sul punto v. PECORELLA, DOVA, *Profili penali delle truffe* on-line, cit., 799.

[286] Cfr. Cass. pen., 19 marzo 2013, n. 28703, in *C.E.D Cass.*, rv. 256348, richiamata in nota da ANTOLISEI, *Manuale di diritto penale,* cit., 475.

[287] Sul punto v. Cass. pen., 20 gennaio 1988, in *Riv. pen. 1989*, 237, richiamata in nota da ANTOLISEI, *Manuale di diritto penale,* cit., 476.

Infatti, le situazioni più comuni sono quelle in cui il truffatore mette in vendita un bene ovvero offre un servizio al fine di ottenere in tutto o in parte il pagamento dello stesso, scomparendo subito dopo senza inviare il bene o prestare il servizio[288].

In gran parte dei casi l'agente realizza l'attività truffaldina contestualmente ad una regolare attività commerciale, oppure creando un'apparente attività commerciale lecita[289]. I soggetti dediti alla commissione di questo tipo di reati rientrano in diverse categorie, trattandosi non solo di criminali abituali, ma anche occasionali, e molto spesso di vere e proprie associazioni per delinquere operanti sul territorio nazionale ed internazionale.

Normalmente le truffe *on-line* hanno ad oggetto importi poco elevati e vengono ripetute con una certa frequenza, al fine di consentire all'agente di accantonare volta per volta una parte del profitto finale[290].

Non di rado i cybercrimali approfittano di un contesto di per sé illecito, e dunque ancor più pericoloso della comune piattaforma di *e-commerce,* per porre in essere le truffe *on-line* a danno dei cyberconsumatori: tale ambito è quello degli *on-line criminal markets*[291], comunemente definiti come la riedizione moderna del mercato nero reale. Il trionfo del commercio illegale sul *dark web*[292] è dovuto

[288] CEDROLA, *I reati informatici: le truffe* on-line, in *www.iusinitinere.it,* 18 gennaio 2017; inoltre, v. Cass. pen, sez. II, 20 dicembre 2019, n.51551, in *C.E.D Cass*., rv. 278231-01, secondo cui: «integra il delitto di truffa contrattuale, ai sensi dell'art. 640 cod. pen., la condotta di messa in vendita di un bene su un sito internet accompagnata dalla sua mancata consegna all'acquirente dopo il pagamento del prezzo, posta in essere da parte di chi falsamente si presenti come alienante ma abbia il solo proposito di indurre la controparte a versare una somma di denaro e di conseguire, quindi, un profitto ingiusto».

[289] SCOPINARO, *Internet e reati contro il patrimonio,* cit., 164.

[290] V. CEDROLA, *I reati informatici: le truffe online*, cit.

[291] Il *trading* sul mercato nero è in continua evoluzione, si tratta di un fenomeno diffuso, sistemico e ben organizzato. Nel 2017 è stato sequestrato, e poi chiuso, uno dei principali *marketplaces* denominato *Alphabay*; esso consentiva la compravendita di numerosi beni o servizi illeciti come sostanze stupefacenti o oggetti rubati, il cui pagamento era consentito solo per mezzo di valute virtuali. La commercializzazione di beni o servizi illegali nel *dark web* continua ad essere una priorità per *l'Europol.*

[292] Il *darkweb* è una componente del *deep web*, e più precisamente è la c.d. "parte oscura "di *internet*. Essa richiede *browser* specifici per la navigazione, come *Tor*, ed è in questa dimensione che si realizza gran parte dell'attività criminale. All'utente è consentita la navigazione mediante un IP nascosto, garantendogli così l'anonimato. I contenuti non possono essere indicizzati dai motori di ricerca ordinari, anche in ragione del fatto che nella maggior parte dei casi essi hanno natura illegale; tuttavia, non si esclude l'utilizzo del *dark web* per fini leciti, quando ad esempio vi sono informazioni che volontariamente sono tenute nascoste per ragioni *privacy*. Ad ogni modo, la navigazione nel *dark web* di per sé non costituisce reato, poiché l'eventuale contingibilità di delitti dipende dal tipo di attività criminosa posta in essere.

senz'altro ad indiscutibili vantaggi riservati ai cybercriminali, in ragione dell'anonimato accordato dai *browser* di navigazione e dell'utilizzo di valute virtuali, nonché della desensibilizzazione soggettiva nell'acquisto dei beni o servizi illeciti con la protezione dell'anonimato, e dell'opportunità di ordinare a distanza, ovverosia senza l'esigenza di un incontro fisico con il rivenditore.

Sebbene siano state sviluppate sofisticate tecniche d'indagine, l'oscuramento dell'indirizzo IP dei soggetti coinvolti, nonché la continua evoluzione del fenomeno rendono particolarmente complessa l'individuazione dei colpevoli, e dunque il contrasto al *trading* illecito sul *dark web*. Inoltre, per fronteggiare efficacemente il suddetto fenomeno risulta decisiva la collaborazione tra le autorità investigative internazionali, nonché la regolazione in materia di valute virtuale, promuovendo così l'emersione di capitali illeciti e la graduale abolizione della barriera dell'anonimato.

Nell'*e-commerce* il filtro informatico causa la dematerializzazione della fase delle trattative, causando non poche conseguenze sia sul piano pratico che giuridico, aumentando così il rischio di errori, fraintendimenti e incertezze circa i termini dell'accordo contrattuale, l'oggetto della vendita e la parte contraente, nonché la conseguente possibilità di realizzazione più facilmente fenomeni frodatori[293].

Tali difficoltà rilevano chiaramente in tutti i casi in cui un soggetto si serva del proprio sito *web* per promuovere un bene, divenendo ancor più pungenti nel caso in cui tra il venditore e l'acquirente si intrometta anche una struttura esterna, come ad esempio un sito di aste.

Sulla base del classico *iter* commerciale *on-line*, l'acquirente, dopo aver individuato un bene o un servizio, contatta il venditore per raggiungere l'accordo, procedendo al pagamento anticipato tramite bonifico bancario o postale, carta di credito, assegno o ricarica di carte prepagate. Dopo aver ricevuto la somma convenuta, il venditore è tenuto ad inviare il bene al destinatario indicato ovvero ad erogare il servizio prescelto. Tuttavia, alcuni venditori consentono il pagamento al momento della consegna del prodotto tramite titoli di credito o contanti.

[293] In argomento v. CIPOLLA, E-commerce *e truffa*, cit., 2625.

La patologia del rapporto può presentarsi a *latere promittentis*, quando vi è la fornitura di un bene diverso, di un pacco vuoto ovvero la mancata spedizione, o a *latere solventis*, nel caso dell'insolvenza *tout court*, del pagamento con carte di credito illegittimamente tenute o dell'emissione di assegni falsificati[294].

Ad ogni modo, la questione d'interesse riguarda principalmente le situazioni in cui la negoziazione assume un carattere criminoso dall'inizio, ravvisandosi elementi frodatori già nel momento della divulgazione pubblicitaria o delle successive trattative. Inoltre, è bene precisare che, benché nella gran parte delle ipotesi la truffa *on-line* avvenga con riguardo al diffuso contratto di compravendita, essa può colpire anche forme contrattuali differenti, inerenti, ad esempio, alla locazione, assicurazione ecc.

«La tipologia più diffusa di accordo commerciale "sospetta" di frode è scandita nelle fasi seguenti: iscrizione ad un sito *e-commerce*, proposta di vendita di un bene di fatto indisponibile, aggiudicazione a colui che palesa interesse, percezione del prezzo […], omissione dell'invio del prodotto offerto, irreperibilità del promittente. Secondo una variante, il venditore pubblicizza le sue offerte mediante un proprio sito *internet*, invitando a comunicare le adesioni a mezzo posta elettronica. […] Secondo una ulteriore variante, tra l'aggiudicazione e il pagamento del prezzo intercorrono contatti tra afferente e acquirente a mezzo telefonico o per il tramite della posta elettronica, in cui il primo garantisce l'esistenza, la qualità e il prezzo modico della res offerta, ne esalta le caratteristiche e precisa tempi e modalità della *solutio*»[295].

Si ritiene sussistere il raggiro, quale elemento essenziale del reato di truffa *ex* art. 640 c.p., in tutti i casi in cui il venditore già al momento della pubblicizzazione del prodotto affermi l'esistenza di qualcosa che in realtà non c'è, traendo in inganno l'acquirente e inducendolo a concludere un contratto di compravendita sulla base di rassicurazioni esplicite anche a mezzo telefonico o via e-mail, circa il particolare valore della res e la convenienza dell'offerta, assicurando altresì l'immediata e rapida spedizione del bene.

[294] *Ivi*, 2625, s.
[295] *Ivi*, 2626.

Inoltre, non di rado il cybercriminale sceglie di servirsi del linguaggio non verbale, o comunque di riferimenti impliciti per ingannare l'acquirente, ad esempio allegando all'offerta fotografie fallaci del bene, o rinviando ad appositi siti *web* che supportano la sua affidabilità.

Ad ogni modo, non è necessario che il venditore faccia riferimento, esplicitamente o implicitamente, all'esistenza del bene o alla vantaggiosità della proposta, poiché è sufficiente che questo si attribuisca, direttamente o indirettamente, qualità che lo rendano credibile ovvero predisponga un contorno di elementi funzionali a definire una situazione apparentemente diversa dalla realtà: in tal caso si tratta più propriamente di artifici idonei ad integrare il delitto di truffa.

Un particolare caso di vendita *on-line* si verifica quando l'offerta telematica ha ad oggetto beni di cui il venditore non dispone al momento della pubblicizzazione, e la suddetta offerta non è corredata di promesse né assistita da successive rassicurazioni o false prospettazioni: si parla a tal proposito di vendita "asettica"[296] a mezzo *internet* di *res* indisponibile.

In tal caso, la mancata spedizione della *res* condurrebbe a ritenere che il fatto integri un'ipotesi di mero inadempimento doloso, precludendo così la responsabilità penale dell'agente in ragione dell'assenza di precedenti contatti di natura decettiva, ossia artifici o raggiri, essenziali per la sussistenza del reato di truffa. Secondo quest'opinione si dovrebbe pertanto concludere nel senso che l'agente, non affermando l'esistenza o la disponibilità della cosa, ed omettendo quindi l'assenza della stessa, nonché la sua intenzione di non spedirla, non realizzerebbe in alcun modo artifici o raggiri, e dunque il fatto non potrebbe integrare il delitto *ex* art. 640 c.p.[297]. Tuttavia, la tesi dell'irrilevanza penale della condotta del venditore che ha offerto un bene tacendone l' indisponibilità non può essere condivisa in ragione del fatto che l'opinione maggioritaria ritiene che anche il silenzio e la reticenza «possano integrare il delitto di truffa, laddove esista in capo al soggetto agente un preciso obbligo giuridico di comunicazione, ovvero laddove

[296] *Ivi*, 2627, ove è definita asettica perché «[…] scevra *ab initio* da palesi menzogne e non seguita da contatti di natura decettiva, né da qualsivoglia spedizione[…]».

[297] Ivi, 2628: «La tesi trova conforto nel fatto che né il diritto né la prassi impongono al commerciante di detenere, già al momento della proposta, l'oggetto pubblicizzato».

venga leso il generale principio di buona fede»[298]; infatti, in tale preciso contesto rileva l'obbligo giuridico di carattere generale di cui all'art. 1337 c.c.[299], che può essere riassunto nel c.d. "principio di buona fede".

In tutti i casi di *e-commerce* la distanza tra venditore e acquirente, nonché il differimento temporale tra promessa, consenso e consegna costringono il consumatore a fidarsi totalmente del venditore e, in un tale contesto di affidamento indifeso dell'acquirente, il principio di buona fede obbliga l'esercente a comunicare anche la più piccola variazione contrattuale. Da ciò si deduce che «in quell'ambito commerciale il silenzio sull'inesistenza della *res* al momento dell'offerta deve essere certamente valutato alla stregua di raggiro: infatti viola il richiamato obbligo generale di comunicazione e altera il modo rilevante quella aspettativa di certa consegna – dato essenziale nella valutazione della convenienza dell'affare»[300].

Quanto sin qui detto trova ulteriore conferma negli art. 22 e 23 del Codice del consumo, dai quali si desume l'importanza che il legislatore ha inteso conferire alla disponibilità del bene oggetto della negoziazione, già al momento dell'offerta, dato che il dovere di lealtà commerciale, come precisato dal Codice del consumo, obbliga l'esercente a segnalare in anticipo le problematiche relative alla disponibilità presente o futura del bene proposto, poiché «la reticenza sul punto è antidoverosa, ingannevole, decettiva, in una parola integra raggiro ai sensi dell'art. 640 c.p.»[301].

---

[298] Cfr. MARTONE, *Il delitto di truffa,* cit., 152; v. anche Cass. pen., Sez. VI, 27 marzo 2019, n. 13411, in *C.E.D. Cass.*, rv. 275463-04: «in tema di truffa contrattuale, anche il silenzio maliziosamente serbato su circostanze rilevanti ai fini della valutazione delle reciproche prestazioni da parte di colui che abbia il dovere di farle conoscere, integra l'elemento del raggiro, idoneo ad influire sulla volontà negoziale del soggetto passivo».

[299] Cfr. CIPOLLA, E-commerce *e truffa,* cit., 2629 s.: «[…]l'art. 1337 c.c. impone alle parti, nella fase delle trattative, un obbligo di lealtà e veridicità, che si traduce nel dovere di informare la controparte sugli elementi di giudizio essenziali per la formazione del convincimento negoziale[…]. […] quando l'obbligo di informare risulta particolarmente ampio, deve considerarsi illecita – perché contraria a buona fede – ogni reticenza sulla difformità tra il reale e l'*id quod plerumque accidit* […]».

[300] Cfr. CIPOLLA, E-commerce *e truffa,* cit., 2630.

[301] *Ivi*, 2631; in argomento v. anche art. 22, comma 1, Codice del consumo: «è considerata ingannevole una pratica commerciale che nella fattispecie concreta, tenuto conto di tutte le caratteristiche e circostanze del caso, nonché dei limiti del mezzo di comunicazione impiegato, omette informazioni rilevanti di cui il consumatore medio ha bisogno in tale contesto per prendere una decisione consapevole di natura commerciale e induce o è idonea ad indurre in tal modo il consumatore medio ad assumere una decisione di natura commerciale che non avrebbe altrimenti preso»; art 22, comma 4, lett. a del Codice del consumo: «nel caso di un invito all'acquisto sono

Ulteriore conferma, nel contesto digitale, della rilevanza penale ai sensi dell'art. 640 c.p. dell'offerta di cose di cui non sia espressa l'indisponibilità, quand'anche manchino profili ingannatori di altro tipo, è data dai regolamenti di utilizzo dei siti di *e-commerce*, i quali non solo tutelano l'aspettativa dei consumatori circa la disponibilità dei beni commercializzati, ma sostengono altresì l'antigiuridicità della dannosa reticenza al riguardo[302].

Nell'ambito della presente trattazione non si può non considerare altresì la questione relativa alla responsabilità dell'*internet service provider*[303] per il commercio fraudolento altrui. Più precisamente, ci si è chiesti se il gestore della piattaforma informatica, per mezzo della quale si realizzano transazioni *on-line* di natura fraudolenta, possa essere considerato penalmente responsabile per omissione, ai sensi dell'art. 40, comma 2, c.p., in concorso con l'autore del fatto, secondo quanto disposto dall'art. 110 c.p., allorché si ravvisino molteplici lamentele, nonché *feedback* negativi inerenti all'attività di un venditore truffaldino.

La suddetta problematica si ripropone costantemente in ragione del fatto che gli autori delle truffe sono difficilmente identificabili, poiché sono soliti comunicare al *provider* false informazioni circa la loro identità, ovvero si servono della rete *wi-fi* per inserirsi in flussi di comunicazioni altrui, e dunque le vittime ricercano altri

considerate rilevanti, ai sensi del comma 1, le informazioni seguenti, qualora non risultino già evidenti dal contesto: a) le caratteristiche principali del prodotto in misura adeguata al mezzo di comunicazione e al prodotto stesso»; art. 23, comma 1, lett. e: «sono considerate in ogni caso ingannevoli le seguenti pratiche commerciali: […] e) invitare all'acquisto di prodotti ad un determinato prezzo senza rivelare l'esistenza di ragionevoli motivi che il professionista può avere per ritenere che non sarà in grado di fornire o di far fornire da un altro professionista quei prodotti o prodotti equivalenti a quel prezzo entro un periodo e in quantità ragionevoli in rapporto al prodotto, all'entità della pubblicità fatta del prodotto e al prezzo offerti».

[302] Sul punto v. CIPOLLA, E-commerce *e truffa*, cit., 2633.

[303] V. PECORELLA, DOVA, *Profili penali delle truffe* on-line, cit., 809 s., secondo cui è bene premettere che la responsabilità del *provider* varia in base all'attività concretamente svolta; le categorie di prestatori di servizi indicate dalla Direttiva 2000/31/CE ad oggi risultano in un certo qual modo inadatte, in ragione della continua evoluzione della realtà digitale, infatti nessuna delle tre tipologie di attività – *mere conduit, caching, ed hosting*– sembra corrispondere pienamente a quella concretamente posta in essere dalle piattaforme di *e-commerce*, sebbene quella che più si avvicini sembra essere quella di *hosting*. Il *provider* può essere responsabile per reati commessi con la propria condotta, ovvero, talvolta, può essere chiamato a rispondere per reati realizzati da altri mediante la sua struttura. Inoltre, v. INGRASSIA, *Il ruolo dell'ISP nel cyberspazio: cittadino, controllore o tutore dell'ordine?* in *Dir. pen. cont*., 8 novembre, 2012, 5 ss.: nel caso di specie, quindi, i gestori delle piattaforme di *e-commerce* sono qualificati come *hosting provider* attivi poiché non sono meri spettatori dei contratti ivi conclusi: per approfondire maggiormente sull'argomento; v. anche ACCINNI, *Profili di responsabilità penale dell'*hosting provider *"attivo"*, in *Arch. pen.*, 2017, 2, 2 ss.

centri d'imputazione della responsabilità, più facilmente individuabili e aggredibili a livello patrimoniale[304].

Una tale responsabilità del *provider* potrebbe essere negata in ragione dell'assenza di un dovere giuridico di impedimento, ad esso riferibile, di vendite fraudolente e account truffaldini[305]. La dottrina, infatti, è orientata ad escludere la presenza di un obbligo generale di sorveglianza delle informazioni trasmesse e memorizzate in capo al gestore, poiché detto obbligo non risulta essere previsto né dal d.l. n. 72/2004, né dalla Direttiva 2000/31/CE, né tantomeno dal d.lgs. n. 70/2003 che, al contrario, all'art. 17, comma 1, dispone espressamente che «nella prestazione dei servizi di cui agli articoli 14, 15 e 16 il prestatore non è assoggettato ad un obbligo generale di sorveglianza sulle informazioni che trasmette o memorizza, né ad un obbligo generale di ricercare attivamente fatti o circostanze che indichino la presenza di attività illecite».

Oltretutto l'eventuale previsione di un dovere del tipo suindicato, si risolverebbe in un potere di censura preventiva sulle informazioni, contrastando così con l'art. 15 della Costituzione che vieta l'intromissione nella corrispondenza e nella comunicazione altrui.

Tuttavia, è bene considerare l'art. 17 del d.lgs. 70/2003 nella sua completezza, poiché ai commi 2 e 3 è disposto che, fatte salve le previsioni di cui agli art. 14, 15 e 16, il gestore che abbia consapevolezza di attività o informazioni illecite debba informare senza ritardo l'autorità giudiziaria o amministrativa con funzioni di vigilanza, e fornire alle autorità competenti che ne facciano richiesta le informazioni funzionali all'individuazione del destinatario dei suoi servizi con cui abbia accordi di memorizzazione di dati, affinché si possa prevenire la realizzazione di attività criminose; inoltre, il *provider* è considerato civilmente responsabile del contenuto dei servizi qualora, a seguito di richiesta da parte dell'autorità giudiziaria o amministrativa, non abbia provveduto ad impedire l'accesso a tale contenuto,

[304] In argomento v. CIPOLLA, E-commerce *e truffa,* cit., 2636.

[305] V. CIPOLLA, E-commerce *e truffa,* cit., 2636: siffatta responsabilità potrebbe escludersi, secondo parte della dottrina anche «sulla base della asserita generale inapplicabilità dell'art. 40 comma 2 c.p. al delitto di truffa, in quanto reato di evento a forma vincolata, oppure in considerazione della rilevanza causale della inerzia degli acquirenti, avvisati sulla condotta del venditore truffaldino[…]»; al contrario, la giurisprudenza più volte si è espressa a favore dell'applicabilità dell'art. 40 c.p. in caso di truffa.

ovvero laddove non abbia informato l'autorità competente della natura illecita o pregiudizievole per un terzo del contenuto di un servizio a cui assicura l'accesso e di cui abbia avuto conoscenza. Di conseguenza, quindi, non può negarsi l'esistenza di un obbligo di impedimento del reato di truffa in capo al *provider*, ma con la precisazione che questo è subordinato alla conoscenza della presunta illeceità di attività o informazioni relative ad un destinatario dei suoi servizi.

Inoltre, al gestore è attribuita la qualifica di intermediario nelle vendite, con conseguente assunzione dell'obbligo giuridico di impedire fatti criminosi ai sensi dell'art. 1759 c.c., in tutti i casi in cui consenta ai venditori di servirsi di appositi strumenti di valorizzazione, funzionali ad incentivare le vendite, tra i quali ad esempio si ravvisa il sistema di *feedback*[306].

Ad ogni modo, alla luce di quanto sin qui detto, sebbene sia possibile ipotizzare l'esistenza di una posizione di garanzia in capo *provider* – a condizione che questo abbia avuto conoscenza dell'attività illecita di un destinatario dei suoi servizi, ed abbia avuto, di fatto, la possibilità di accedere al contenuto dei messaggi –, potrebbe comunque negarsi in concreto la responsabilità omissiva del gestore, adducendo l'inesistenza di un contributo causale alla realizzazione di vendite frodatorie, nonché la mancanza del requisito soggettivo doloso. Tra l'altro, il gestore non difficilmente potrebbe obiettare l'impossibilità di accertare preventivamente l'eventuale natura illecita dei contenuti inseriti in rete da terzi[307].

Dunque, «pur ammessa (a certe condizioni) l'esistenza *de iure condito* di una posizione di garanzia, potrebbe ravvisarsi in capo al *service provider* c.d. *mere conduit*, o all' *host provider* una responsabilità di tipo omissivo *ex* art. 40 comma 2 c.p. solo allorché il *service provider* sia stato formalmente diffidato a rimuovere dalla rete l'attività illecita e non vi abbia provveduto; in tali casi la volontaria omissione contribuirebbe alla prosecuzione dell'offesa al bene giuridico tutelato, favorendo l'innalzamento del rischio di trasmissione di contenuti illeciti»[308].

In conclusione, sembrerebbe opportuno valutare singolarmente le situazioni, tenendo conto della tipologia di attività posta in essere dal *provider* e della reale percepibilità dell'illeceità dei contenuti immessi nel *web*.

---

[306] *Ivi*, 2637.
[307] In argomento v. CIPOLLA, E-commerce *e truffa*, cit., 2638.
[308] *Ibidem*.

2.2.4 Il *locus commissi delicti* nelle truffe *on-line*

La corretta individuazione del momento consumativo del reato di truffa commesso *on-line* è fondamentale per la risoluzione della questione relativa alla determinazione del *locus commissi delicti* e del giudice territorialmente competente in materia.

Come anticipato, secondo quanto sostenuto dall'orientamento attualmente prevalente, affermatosi a partire da una sentenza delle Sezioni Unite della fine degli anni '60[309], la consumazione del reato di cui all'art. 640 c.p. si verifica con la definitiva *deminutio patrimonii* per il soggetto passivo e con il relativo conseguimento dell'ingiusto profitto per il soggetto agente o per un terzo; tale convinzione, peraltro, appare del tutto coerente con la natura di reato di danno, propria della truffa, che risulterebbe stravolta qualora si ritenesse già consumato il delitto in presenza dell'assunzione da parte del soggetto passivo di un formale obbligo di dare[310].

Trattandosi di un reato a doppio evento consumativo, nei casi in cui esso si realizzi *on-line*, in virtù delle tipicità proprie del contesto digitale – prima fra tutte la mancanza di contatto tra le parti –, potrebbero porsi non pochi problemi circa la determinazione del momento consumativo e del *locus commissi delicti*. Ad esempio, talvolta, le criticità riguardano lo "scollamento temporale" dei due eventi, quali il danno patrimoniale e l'ingiusto profitto, divenendo così necessario interrogarsi su quale dei due debba essere valorizzato per i fini suddetti.

Tuttavia, è bene precisare che quella dell'identificazione del *locus commissi delicti* è una questione che si pone a prescindere dall'eventuale contestualità o meno della realizzazione degli eventi funzionali ad integrare il momento consumativo del reato di truffa *on-line*, in ragione delle caratteristiche del non-luogo informatico.

È chiaro che in caso di coincidenza dei due eventi suindicati non si rileva alcuna difficoltà a proposito dell'individuazione del momento consumativo del reato, limitandosi la questione alla determinazione del *locus commissi delicti*;

---

[309] Sul punto v. PECORELLA, *Truffe* on-line*: momento consumativo e competenza territoriale, in Dir. pen. cont*., 10 maggio 2012, 8, che richiama Cass. pen., Sez. Un., 22 marzo 1969, P.m. c. Carraro e altri, in *Foro it*., 1970, 2, 5 ss. con nota di BOSCHI, e Cass. pen., Sez. Un., 30 novembre 1974, Forneris, in *Cass. pen.*, 1975, 751 ss.

[310] V. PECORELLA, *Truffe* on-line*: momento consumativo e competenza territoriale*, cit., 11.

eppure, nella gran parte delle situazioni delittuose che si realizzano *on-line*, specie in occasione di transazioni commerciali su piattaforme telematiche, emerge il suddetto scollamento temporale, ovverosia una discrasia cronologica tra l'evento di danno e l'evento di profitto, che rende difficoltosa la determinazione del momento consumativo e conseguentemente del *locus commissi delicti*[311].

Con riguardo alle truffe *on-line*, la problematica relativa all'individuazione del *tempus* e del *locus commissi delicti* è stata affrontata con particolare riferimento alle ipotesi in cui un soggetto, a seguito di artifici e raggiri, sia stato ingannato ed abbia effettuato il pagamento di beni acquistati e mai ricevuti tramite ricariche di carte *Postepay*.

A tal proposito si ravvisano due diversi orientamenti interpretativi: il primo riconosce il *locus commissi delciti* nel luogo in cui è stato posto in essere il pagamento che comporta l'immediato nocumento patrimoniale per la vittima; il secondo, al contrario, tiene conto del luogo di destinazione del pagamento. Siffatta ultima tesi apparirebbe coerente con la natura e la struttura della fattispecie, poiché il reato di truffa può dirsi perfezionato solo con l'effettivo conseguimento del vantaggio patrimoniale per l'agente da cui derivi la definitiva *deminutio patrimonii* per la vittima[312].

L'accertamento concernente il luogo di conseguimento dell'ingiusto profitto dipende dalle peculiarità dello strumento di pagamento *Postepay*, il quale permette al titolare di eseguire operazioni di prelievo e pagamento, anche *on-line*, compatibilmente con l'importo disponibile; si tratta di una carta prepagata non necessariamente abbinata ad un conto corrente che può essere utilizzata presso qualunque punto convenzionato. Alla luce di ciò, il suddetto luogo di ottenimento del vantaggio patrimoniale finirebbe col coincidere con quello di concreta utilizzazione della carta, e dunque con gli sportelli ATM o con il domicilio del reo in considerazione del fatto che si tratta di un mezzo di pagamento usato soprattutto *on-line*.

[311] Sul punto v. MARZULLO, *Truffa informatica*, cit., 6.

[312] In argomento v. FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in CADOPPI, CANESTRARI, MANNA, PAPA (diretto da), Cybercrime, Torino, 2019, 164.

Ebbene, una simile conclusione rende complicata, se non impossibile, la determinazione del giudice competente per mezzo del criterio previsto dall'art. 8 c.p.p., e sceglie di considerare uno dei criteri suppletivi *ex* art. 9 c.p.p., e più precisamente quello fondato sul luogo di residenza domicilio o dimora del soggetto attivo[313].

Tuttavia, la Procura generale presso la Corte di Cassazione, come sottolineato da autorevole dottrina, accorda rilevanza al luogo in cui si realizza il nocumento per la vittima, ovverosia al luogo di ricarica della carta prepagata, e non a quello in cui si ottiene il profitto, risolvendosi così la problematica in questione.

Inoltre, di recente la Corte di Cassazione ha affermato che «nel delitto di truffa, quando il profitto è conseguito mediante accredito su carta di pagamento ricaricabile (nella specie "*Postepay*"), il tempo e il luogo di consumazione del reato sono quelli in cui la persona offesa ha proceduto al versamento del denaro sulla carta, poiché tale operazione ha realizzato contestualmente sia l'effettivo conseguimento del profitto da parte dell'agente, che ottiene l'immediata disponibilità della somma versata, e non un mero diritto di credito, sia la definitiva diminuzione patrimoniale in danno della vittima»[314].

Nel caso in cui il pagamento dovesse essere effettuato dalla vittima a mezzo di bonifico bancario si dovrebbe applicare un criterio diverso da quello suesposto, in ragione delle differenti tempistiche di accredito, e della mancata immediatezza tipica della ricarica Postepay. Più precisamente con riguardo al bonifico bancario, la Procura generale presso la Corte di Cassazione valorizza il momento e il luogo in cui l'agente consegue il profitto, quale risultato della condotta frodatoria da lui eseguita, poiché diversamente, si realizzerebbe un'anticipazione del momento consumativo del reato[315].

Qualora il pagamento fosse compiuto con titoli di credito, in base a quanto sostenuto dall'orientamento prevalente, si dovrebbero favorire il momento e il

---

[313] V. PECORELLA, *Truffe* on-line*: momento consumativo e competenza territoriale,* cit., 2.

[314] Cfr. FLOR, *La legge penale nello spazio,* cit., 165 che richiama in nota Cass. pen., 6 ottobre 2017, n. 3329.

[315] *Ivi*, 165 s; v. anche Cass. pen., sez. II, 20 ottobre 2016, n. 48027, in *www.penale.it;* in argomento v. anche DI PRISCO, *Truffe* online *e Postepay: quando e dove si consuma il reato?*, in *www.iusinitinere.it*, 29 gennaio 2018.

luogo di riscossione del titolo stesso, e non quelli in cui si rinviene la sua disponibilità[316].

Dal punto di vista processuale, assumono particolare importanza, ai fini dell'individuazione del *locus commissi delicti* e del giudice territorialmente competente, i criteri residuali *ex* art. 9 c.p.p., in virtù delle difficoltà applicative, dovute alle tipicità del *web*, della regola generale di cui all'art. 8 c.p.p.

Al di là delle osservazioni sin qui esposte permangono non poche incertezze circa la determinazione del *locus commissi delicti* nelle truffe *on-line,* poiché si tratta di una questione fortemente connessa alle modalità di manifestazione della condotta, ragion per cui non può definirsi un principio generale in materia.

2.2.5 La truffa *on-line* e i rapporti con le altre figure delittuose

A questo punto della trattazione è senz'altro opportuno considerare i rapporti intercorrenti tra il reato di truffa *on-line ex* art. 640 c.p. e le altre figure delittuose, soffermando l'attenzione sul rapporto con i delitti di insolvenza fraudolenta *ex* art. 641 c.p. e di frode in commercio *ex* art. 515 c.p., nonché con i reati di sostituzione di persona *ex* art. 494 c.p. e accesso abusivo ad un sistema informatico o telematico *ex* art. 615-*ter* c.p., che verranno ripresi più dettagliatamente in occasione dell'esame del fenomeno del *phishing*; si rinvia, invece, ad un momento successivo l'analisi relativa al rapporto con il delitto di frode informatica *ex* art. 640-*ter* c.p., ritenendosi indispensabile una previa definizione della figura *criminis.*

La complessa questione relativa al confine tra il delitto di truffa e quello di insolvenza fraudolenta si fonda sul fatto che la condotta di dissimulazione dello stato di insolvenza corrisponde a grandi linee a quella del soggetto che offre in vendita beni di cui tace l'indisponibilità, senza aggiungere altro. Pur volendo ammettere un'interpretazione estensiva del reato di cui all'art. 641 c.p. al fine di ricomprendere nel concetto di insolvenza anche il "non possesso" del bene oggetto della vendita, non si potrebbe comunque configurare il reato di insolvenza fraudolenta nel caso di vendita asettica, in ragione del fatto che nell'art. 641 c.p. si rileva nel soggetto passivo più uno stato di ignoranza che di errore indotto, e anche

[316] Sul punto v. FLOR, *La legge penale nello spazio,* cit., 166.

perché l'impegno assunto dal venditore non sembra essere ricompreso nell'insieme delle obbligazioni a cui si riferisce la norma considerata[317].

La *ratio* fondante l'art. 641 c.p. è volta a punire il soggetto che approfitta di convenzioni sociali e commerciali che convincono ad avere fiducia nella condotta altrui: in questa prospettiva, l'art. 641 c.p. può essere applicato solo con riguardo a quelle obbligazioni in cui il soggetto attivo ha l'opportunità di trarre un ingiusto vantaggio da una posizione di inferiorità, non risultante dalla libera scelta, ma obbligata dall'esigenza di accordare fiducia all'altro contraente[318].

Dunque, non sembra esservi alcuna alternativa, poiché la condotta di un soggetto che offre in vendita, su un sito *e-commerce*, un bene o un servizio, tacendone l'indisponibilità ed omettendo l'adempiemmo dell'obbligazione assunta a fronte del pagamento effettuato dall'acquirente, integra il delitto di truffa e non quello di insolvenza fraudolenta.

Nel caso in cui l'alienazione della *res* indisponibile dovesse concludersi con la consegna all'acquirente di un bene differente da quello promosso dal venditore non potrebbe configurarsi il reato di frode in commercio di cui all'art. 515 c.p., poiché tale figura criminosa ai fini della sua realizzazione richiede che la consegna *aliud pro alio* non sia anticipata da artifici o raggiri[319], mentre nel caso di specie la suddetta consegna risulta essere preceduta da maliziosa reticenza integrante raggiro, dovendosi concludere, dunque, per la configurazione del reato di truffa, con conseguente inapplicabilità dell'art. 515 c.p.

---

[317] Sul punto v. CIPOLLA, E-commerce *e truffa,* cit., 2633 s.

[318] *Ivi*, 2634.

[319] In argomento v. CIPOLLA, E-commerce *e truffa,* cit., 2634 che richiama Cass. pen., Sez. II, 22 maggio 1976, Mattioli, in *C.E.D Cass.*, rv. 133628. Al contrario, secondo SCOPINARO, *Internet e reati contro il patrimonio,* cit., 178, non è corretto ritenere che nella fattispecie di cui all'art. 515 c.p. «manchi l'elemento dell'artificio o raggiro con induzione in errore del soggetto, con la conseguenza che la frode in commercio consisterebbe in un reato diverso da quello di truffa e, quindi, applicabile sempre in caso concreto; oppure, che tale elemento sia ravvisabile solo in presenza di un comportamento attivo da parte del commerciante, ulteriore rispetto al fatto di esercitare una attività legittima e che appare come tale […]. Con la conseguenza, in tale seconda ipotesi, che la fattispecie lascerebbe il posto alla truffa solo in presenza di tale comportamento positivo». L'autore, inoltre, sulla possibilità che la truffa *on-line* concorra con la frode in commercio, ritiene che la questione del concorso apparente debba essere risolta in favore della truffa, «essendo la frode in commercio fattispecie speciale rispetto ad essa sia rispetto alla condotta, sia rispetto all'evento, in forza di quanto disposto dalla stessa art. 515 c.p. il quale prevede che il soggetto sia punito qualora il fatto non costituisca più grave delitto».

Non di rado i cybercrimnali si servono dell'identità altrui per porre in essere azioni criminose, tra le quali la truffa a mezzo *web*. Premesso che a ciascun soggetto è riconosciuta la libertà di attribuirsi in rete l'identità che preferisce, la condotta del soggetto che si registra su piattaforme telematiche a nome di un'altra persona, inconsapevole, facendo ricadere su di essa gli effetti delle proprie azioni criminose, integra non solo il reato di truffa, a seguito di artifici e raggiri, ma anche quello di sostituzione di persona, poiché viene sfruttata l'identità altrui con il preciso fine di ottenere un vantaggio e causare un danno[320].

Dunque, il delitto di truffa *ex* art. 640 c.p. può formalmente concorrere con il reato di sostituzione di persona di cui all'art. 494 c.p., poiché si tratta di norme funzionali a tutelare due beni giuridici eterogenei, ravvisabili nella fede pubblica e nel patrimonio[321], e in virtù del fatto che la sostituzione di persona non rappresenta un elemento costitutivo della truffa[322].

Si ritiene inoltre configurabile il concorso tra il reato di truffa di cui all'art. 640 c.p. e il delitto di accesso abusivo ad un sistema informatico o telematico *ex* art. 615-*ter* c.p., in virtù della diversità dei beni tutelati.

2.3 Il delitto di frode informatica *ex* art. 640-*ter* c.p.: inquadramento della fattispecie

La frode informatica è una figura delittuosa disciplinata dall'art. 640-*ter* c.p. ed è riconducibile alla categoria generale delle truffe *on-line*; essa è stata introdotta nel Libro II, Titolo XIII, Capo II del codice penale, nell'ambito dei delitti contro il patrimonio mediante frode, dall'art. 10 della Legge n. 547/1993.

È bene precisare già da ora che la norma in esame è stata inserita nel novero dei reati contro il patrimonio – prima ancora che per definire le tipicità del nuovo fenomeno dell'impiego fraudolento di un sistema informatico – per porre fine alla

[320] In argomento v. CIPOLLA, E-commerce *e truffa,* cit., 2636; v. anche MALAGNINO, *Sostituzione di persona e* web*: le false recensioni* online, in *Giur. pen. web*, 2019, 4, 5.

[321] Sul punto v. Cass. pen., Sez. II, 11 settembre 2020, n. 26589, in *C.E.D. Cass.*, rv. 279647-01; v. anche Cass. pen., Sez. V, 19 febbraio 1998, n. 10805, in *C.E.D. Cass*, rv. 211521-01, secondo cui: «sussiste concorso formale si reati tra la truffa e la sostituzione di persona, poiché si tratta della medesima condotta che integra sue ipotesi delittuose diverse e tra loro autonome: ne consegue che lo stesso comportamento ben può realizzare l'elemento materiale di entrambi i reati».

[322] Trib. Milano 19 ottobre 2008, in *Corr. merito* ,2009, 3, 288, con nota di AGNINO, Computer crime *e fattispecie penali tradizionali: quando il* phishing *integra il delitto di truffa*.

disputa sulla configurabilità del delitto di truffa *ex* art. 640 c.p.[323]. La dottrina maggioritaria, infatti, escludeva la sussumibilità del fatto fraudolento nel delitto di cui all'art. 640 c.p., in virtù dell'insuperabilità dei limiti posti dal divieto di analogia in m*alam partem*[324].

Il legislatore nel formulare la fattispecie ha eliminato qualunque riferimento ai requisiti propri della truffa, non solo per distinguere definitivamente i due reati, ma anche perché gli elementi truffaldini risultavano inappropriati rispetto alle modalità esecutive e al contesto digitale di azione. Non sembra dunque condivisibile la tesi secondo cui la frode informatica sarebbe stata costruita sulla falsariga del reato di truffa, dovendosi al contrario affermare l'autonomia strutturale della norma in questione[325].

L'art. 640-*ter* c.p.[326] punisce al primo comma chiunque, alterando in qualunque modo il funzionamento di un sistema informatico o telematico, o

---

[323] Cfr. MINICUCCI, *Le frodi informatiche*, in CADOPPI, CANESTRARI, MANNA, PAPA (diretto da), Cybercrim*e*, Torino, 2019, 828: «[…]la fattispecie era da tempo invocata dai teorici e dai pratici del diritto soprattutto allo scopo di emarginare il dibattito intorno all' applicabilità del delitto di truffa in campo informatico, osteggiata in particolare da chi non riteneva in alcun modo assimilabile all' induzione in errore di un uomo la manomissione e/o l'impiego truffaldino di una macchina».

[324] Per approfondire sul punto v. CAMPEIS, *La frode informatica*, in CENDON (diretto da), *Trattato dei nuovi danni, informazioni erronee, soggetti deboli, illeciti informatici, danni ambientali*, Vol. V, Padova, 2011, 917 s.: nella fase antecedente all'introduzione dell'articolo 640-*ter* nel codice penale non sono mancati tentativi di interpretazione estensiva dell'art. 640 c.p. al fine di ricomprendervi anche le ipotesi di frodi elettroniche; tuttavia, tale interpretazione è stata fortemente criticata in ragione del divieto di analogia *in malam partem*, rendendosi così essenziale la definitiva differenziazione tra i casi in cui l'ingiusto vantaggio fosse ottenuto attraverso l'alterazione della volontà del soggetto agente da quelli in cui l' azione ricadeva direttamente sull'elaboratore elettronico senza alcun coinvolgimento della persona fisica.

[325] Come si avrà modo di precisare in seguito, l'assenza del riferimento all'induzione in errore di un individuo e lo spostamento di ricchezza da un patrimonio all'altro in assenza di un atto di disposizione patrimoniale consapevole priva la fattispecie della natura di reato a cooperazione artificiosa del soggetto passivo, tipica della truffa, accostandola, invece, alla categoria del furto con mezzo fraudolento; v. MINICUCCI, *Le frodi informatiche*, cit., 828, che richiama in nota Cass. pen., 5 febbraio 2009, n. 8755, in *C.E.D. Cass.*, rv. 243238, infatti «sembra difficile spiegare l'affermazione giurisprudenziale secondo cui la frode mantiene medesimi elementi costitutivi della truffa dalla quale si differenzia solamente perché l'attività fraudolenta dell'agente investe non la persona (soggetto passivo), di cui difetta l'induzione in errore, bensì il "sistema informatico" di pertinenza alla medesima, attraverso la manipolazione di detto sistema».

[326] L'art. 640-*ter* c.p. dispone che: «Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico ad esso pertinenti procura a sé o ad altri un in 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. La pena è della reclusione da uno a cinque anni e della multa da trecentonove euro a millecinquecentoquarantanove euro se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema. La pena è della reclusione da due a sei anni e della multa da 600 a euro 3000 se il fatto è commesso con furto o indebito utilizzo dell'identità

intervenendo senza diritto, con qualsivoglia modalità su dati informazioni o programmi presenti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno.

Come si evince dalla collocazione del reato di cui all'art 640-*ter* tra i delitti contro il patrimonio mediante frode, il bene giuridico che il legislatore ha voluto tutelare con la norma in esame è certamente il patrimonio; tuttavia, in dottrina sono emersi diversi orientamenti volti ad ampliare l'oggetto di tutela.

Secondo un primo indirizzo si deve includere anche il corretto funzionamento dei sistemi informatici e la riservatezza che ne deve accompagnare l'utilizzo[327]; un altro approccio ritiene doversi ricomprendere anche la libertà negoziale[328]; mentre secondo un'ulteriore posizione si deve considerare anche il diritto a godere liberamente dello strumento informatico[329].

Ad ogni modo, secondo alcuni autori sarebbe maggiormente convincente la tesi che ravvisa nel patrimonio l'unico oggetto di tutela, dovendosi considerare tutti gli altri beni come strumentali alla tutela patrimoniale[330].

La giurisprudenza, invece, si espressa a favore dell'estensione del bene giuridico, il quale non dovrebbe limitarsi al patrimonio ma considerare anche il regolare funzionamento dei sistemi informatici, la riservatezza dei dati e la certezza e speditezza del traffico giuridico-informatico[331].

Il soggetto attivo del reato di cui all'art. 640-*ter* c.p. può essere "chiunque", infatti si tratta di un reato comune, sebbene il comma secondo contempli una

digitale in sanno di uno o più soggetti. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo e terzo comma o taluna delle circostanze previste dall' art 61, primo comma, numero 5, limitatamente all' aver approfittato di circostanze di persona, anche in riferimento all' età, e numero 7».

[327] Sul punto v. MINICUCCI, *Le frodi informatiche,* cit., 829; ANTOLISEI, *Manuale di diritto penale,* cit., 499; FIANDACA, MUSCO, *Diritto penale. Parte speciale*, Vol. II, 7ª ed., Bologna, 2015, 205 ss.

[328] In argomento v. MINICUCCI, *Le frodi informatiche,* cit., 829; MASI, *Frodi informatiche e attività bancaria*, in *Riv. pen. econ.*, 1995, 4, 427.

[329] Sul punto v. MINICUCCI, *Le frodi informatiche,* cit., 829; AMATO, DESTITO, DEZZANI, SANTORIELLO, *I reati informatici*, Padova, 2010, 104.

[330] V. MINICUCCI, *Le frodi informatiche,* cit., 829; MEZZETTI, *Reati contro il patrimonio*, in GROSSO, PADOVANI, PAGLIARO (diretto da), *Trattato di diritto penale. Parte speciale*, XV, Milano, 2013, 461.

[331] V. MINICUCCI, *Le frodi informatiche,* cit., 829, che richiama Cass. pen., 15 aprile 2011, n. 17748, in *C.E.D. Cass.*, rv. 250113.

circostanza aggravante speciale richiedente, ai fini dell'integrazione, la qualifica di "operatore del sistema".

Secondo quanto sostenuto dalla giurisprudenza, il soggetto passivo del delitto di frode informatica sarebbe il titolare del sistema informatico o telematico, ovvero dei dati, informazioni o programmi in esso elaborati[332].

La norma descrive due condotte alternative, che, anche se realizzate separatamente, sono entrambe idonee a configurare il reato in questione.

La prima condotta fraudolenta consiste nell'alterazione, in qualunque modo, del funzionamento di un sistema informatico o telematico, e dunque in una modifica del corretto svolgimento di un procedimento di elaborazione o trasmissione dei dati; la seconda, invece, si sostanzia nell'intervento non autorizzato, con qualsivoglia modalità, su dati, informazioni o programmi presenti in un sistema informatico o telematico o ad esso pertinente, riferendosi in tal modo a tutte quelle forme di interferenza differenti dall'alterazione del funzionamento del sistema informatico.

Si tratta di un reato a forma libera, e solo apparentemente a forma vincolata, poiché le suindicate condotte possono realizzarsi, in qualunque modo e in qualsivoglia modalità, come si evince dalla descrizione del primo comma[333].

«È richiesto che la condotta materiale incida, dunque, in qualsiasi modo sui meccanismi fisici e logici di funzionamento di un sistema informatico o telematico»[334].

L'alterazione del funzionamento del sistema, che consiste nel causare anormalità nei sistemi presi di mira, può realizzarsi in due modi: o agendo sul *software*, e quindi su programmi, dati o informazioni inseriti e conservati in un apparato con abilità di elaborazione, o operando sull'*hardware*, vale a dire sulle parti materiali, al fine di far svolgere operazioni differenti da quelle per cui la macchina è stata progettata.

---

[332] V. CUOMO, RAZZANTE, *La nuova disciplina dei reati informatici*, cit., 167 secondo cui: «la ricaduta della condotta, in termini meccanicistici, nei confronti dell'elaboratore elettronico fa coincidere il titolare dell'interesse leso con il soggetto sul quale si riverbera il danno».

[333] V. Cass. pen., Sez. V, 24 novembre 2003, n. 4576, in *www.ius-web.it*; v. anche CAMPEIS, *La frode informatica*, cit., 919: «la norma, infatti, presenta una struttura a forma libera, prevedendo in via alternativa le due condotte di alterazione del funzionamento del sistema informatico o telematico ovvero l'attuazione di un intervento non autorizzato, effettuato con qualsiasi modalità, sui dati o programmi ivi contenuti»; v. anche AMATO, DESTITO, DEZZANI, SANTORIELLO, *I reati informatici*, cit.,105.

[334] Cfr. CAMPEIS, *La frode informatica*, cit., 919.

In altre parole, si ravvisa "alterazione del sistema" nei casi in cui si verifichino operazioni di manipolazione dell'elemento fisico – *hardware* – o logico – *software* – del sistema, alle quali sussegua un differente procedimento informatico capace di pregiudicare i risultati ottenuti o di provocare, in ogni caso, la deviazione da un modello tipico[335].

Inoltre, la giurisprudenza ha opportunatamente specificato che l'alterazione del funzionamento di un sistema informatico o telematico riguarda qualunque attività od omissione che, mediante la manipolazione dei dati informatici, influisca sulla normale esecuzione del processo di elaborazione o trasmissione dei dati e, dunque, sia sull'*hardware* che sul *software*[336].

La condotta di alterazione, quindi, si ripercuote sulle modalità di funzionamento del sistema informatico o telematico; tale operazione di manipolazione può giungere fino a modificare le finalità a cui il sistema è preordinato, o limitarsi ad incidere sui contenuti dello stesso nel rispetto della destinazione del sistema[337].

La condotta alternativa "di intervento senza diritto" si riferisce a dati, informazioni o programmi, e quindi a qualsiasi file contenuto nei sistemi informatici o telematici o in supporti ad essi pertinenti, purché siano impiegati in un sistema informatico. Non rileva in alcun modo l'eventualità che i dati non siano oggetto di una prima elaborazione, bensì il risultato di un procedimento in parte eseguito, poiché ciò che conta è la relazione funzionale tra i detti dati e l'elaborazione che permette all'autore di ottenere un ingiusto profitto.

Il riferimento a dati, informazioni o programmi è volutamente ampia, volendosi scongiurare possibili vuoti di tutela.

Inoltre, è opportuno indicare che, con riguardo alla distinzione tra il concetto di "alterazione" e quello di " intervento", parte della dottrina ritiene che il primo costituisca una fase preliminare al secondo, o che addirittura sia una sua mera specificazione; secondo altra parte della dottrina, invece, la distinzione si motiverebbe sulla base del fatto che mentre l'alterazione provoca una modifica fisiologica del sistema, l'intervento non autorizzato si traduce in un'interferenza

[335] In argomento v. MINICUCCI, *Le frodi informatiche*, cit., 832.
[336] V. Cass, pen., Sez II, 6 marzo 2013, n. 13475, in *www.webgiuridico.it*.
[337] V. AMATO, DESTITO, DEZZANI, SANTORIELLO, *I reati informatici*, cit., 105 s.

immediata sul dato, informazione o programma oggetto del processo informatico, variandone così il contenuto e l'esito del processo stesso.

Come espressamente indicato, l'intervento deve essere "senza diritto", vale a dire non autorizzato, abusivo[338]. Tale inciso "senza diritto" può riferirsi sia all'intervento verificatosi senza l'indispensabile consenso del titolare dei dati, informazioni o programmi contenuti nel sistema, sia all'intervento realizzatosi in contrasto con le norme giuridiche dell'ordinamento o con altre fonti.

Mentre nella prima ipotesi, ai fini della realizzazione del reato, è necessaria l'assenza del consenso del titolare di dati, informazioni o programmi, nella seconda ipotesi il reato può configurarsi anche nei confronti di chi, sebbene sia autorizzato ad accedere e a compiere operazioni sul sistema, agisca con finalità illecite[339].

L'opinione più plausibile sembrerebbe essere quella che considera la locuzione ridondante, poiché, trattandosi di un reato finalizzato all'ottenimento di un ingiusto vantaggio con altrui danno, non si dovrebbe attribuire rilevanza alla posizione giuridica assunta dall'agente, non essendo altresì necessario stabilire se questo abbia o meno il diritto di intervenire, ritenendosi, per contro, sufficiente il fatto che l'intervento sia posto in essere con finalità antigiuridiche.

Dunque, il reato di cui all'art. 640-*ter* c.p. esige che la condotta dell'agente sia realizzata con le suindicate modalità fraudolente e che sia diretta ad un sistema informatico o telematico ovvero a dati, informazioni o programmi. A tal proposito, l'oggetto materiale dell'alterazione è il sistema informatico o telematico, mentre quello dell'intervento senza diritto è rappresentato da dati, informazioni o

---

[338] In argomento v. AMATO, DESTITO, DEZZANI, SANTORIELLO, *I reati informatici*, cit.,106 s.: per precisione è bene indicare che alcuni autori ritengono che l'inciso "senza diritto", che letteralmente si riferisce alla sola condotta di intervento, sia da considerarsi rilevante per entrambe le condotte alternative.

[339] Sul punto v. AMATO, DESTITO, DEZZANI, SANTORIELLO, *I reati informatici*, cit., 107; v. anche MINICUCCI, *Le frodi informatiche,* cit., 833 s., il quale con riguardo alle diverse ricostruzioni ermeneutiche sul punto afferma che, secondo una prima tesi, nel caso in cui si ritenesse fondamentale la mancanza dell' autorizzazione per accedere al sistema, si verificherebbe un' ampio vuoto di tutela, nonché *l'interpretatio abrogans* del secondo comma della norma nel punto in cui punisce più pesantemente colui che agisce con la qualifica di operatore del sistema. Si tratterebbe quindi, secondo tale tesi, di una locuzione pleonastica, «descrittiva di una antigiuridicità speciale apparente e legata all' assenza del consenso del titolare *ex* art. 51c.p. (peraltro implicita nella stessa ingiustizia del profitto), o comunque "superata" dalla previsione della condotta manipolativa e dell'evento di profitto», Altra tesi invece sostiene che «l'agente non debba essere munito di alcuna legittimazione ad agire, anche quando egli, pur astrattamente autorizzato, operi per fini illeciti, al di fuori dei contorni del titolo abilitativo». Del resto, anche la giurisprudenza appare divisa sul punto.

programmi[340]; inoltre, non è necessario che l'oggetto materiale della condotta sia "altrui".

Non ravvisandosi una definizione legislativa di "sistema informatico", la giurisprudenza ha elaborato una definizione generale del termine, intendendolo come il complesso di apparecchiature finalizzate a svolgere una qualunque funzione utile all'individuo, mediante l'impiego di tecnologie informatiche, le quali si contraddistinguono per la coesistenza di tre aspetti operativi: la registrazione o memorizzazione su appositi supporti, attraverso impulsi elettronici, di dati costituiti da simboli in svariate combinazioni; l'elaborazione automatica dei suddetti dati ad opera della macchina; l'organizzazione logica degli stessi dati al fine di permettergli di esprimere un significato utile all'individuo[341].

Il sistema telematico, invece, si riferisce a più sistemi informatici tra loro costantemente connessi, via etere o via cavo, con lo scopo di consentire la trasmissione di informazioni a distanza[342].

I dati sono rappresentati da simboli numerici in differenti combinazioni; le informazioni sono costituite da un insieme di dati logicamente organizzati.

Come la truffa, anche la frode informatica è un reato a doppio evento, per cui, ai fini dell'integrazione del reato, è essenziale che si realizzino l'ingiusto profitto e l'altrui danno, dovendo altresì sussistere il nesso causale tra la condotta fraudolenta tenuta dall'agente e gli eventi suddetti[343] ; dunque, il delitto in esame, al pari dell'art. 640 c.p., si perfeziona nel momento in cui si verifica l'ingiusto profitto, per il soggetto attivo o per un terzo, e il danno patrimoniale, per il soggetto passivo. Inoltre, può configurarsi il tentativo del reato in questione in tutti i casi in cui alla condotta frodatoria non dovesse conseguire il duplice evento.

Il profitto deve essere ingiusto ed avere natura patrimoniale e non necessariamente economica; inoltre, esso può essere conseguito sia dall'agente che

---

[340] V. AMATO, DESTITO, DEZZANI, SANTORIELLO, *I reati informatici*, cit., 107.

[341] V. STALLA, *L'accesso abusivo ad un sistema informatico o telematico*, in www.penale.it.

[342] *Ibidem*.

[343] V. AMATO, DESTITO, DEZZANI, SANTORIELLO, *I reati informatici*, cit., 110: «Non può evocarsi, in proposito, la nozione di "atto di disposizione patrimoniale", poiché tale espressione non può che far riferimento ad un atto giuridico involontario del soggetto passivo. Si tratta di nozione tipica della truffa, laddove vi è induzione in errore di una persona fisica. Nell' ipotesi in esame è invece sufficiente che vantaggi e danni dipendano dalla manipolazione del sistema informatico realizzata dal soggetto agente anche se in modo automatico[…]».

da un altro soggetto. Ad ogni modo, ai fini della consumazione del delitto in esame è richiesta la realizzazione anche di un altro evento, quale diretta conseguenza dell'ingiusto vantaggio, ovverosia il danno patrimoniale altrui.

Per quanto riguarda la determinazione del *locus commissi delicti* nel delitto di frode informatica si ripropongono le medesime considerazioni svolte in materia di truffa[344], poiché, parimenti, la fattispecie in esame si intende consumata nel momento in cui l'agente realizza il profitto con altrui danno.

Dunque, al fine di individuare il luogo di commissione del reato, è opportuno considerare il momento e il luogo di conseguimento dell'ingiusto vantaggio con altrui danno, e nel caso in cui non si possa definire il luogo esatto di consumazione, la competenza territoriale viene stabilita in base ai criteri residuali di cui all'art. 9 c.p.p., comma 1 e 2[345].

L'elemento soggettivo richiesto dal reato in esame è il dolo generico, dato che assumono rilevanza la consapevolezza e la volontà dell'agente di porre in essere le suindicate condotte, e di realizzare, mediante esse, un ingiusto profitto per sé o per altri con altrui danno[346].

Il comma secondo dell'articolo 640-*ter* c.p. punisce più gravemente l'agente che pone in essere il reato di frode informatica di cui al comma primo, a danno dello Stato o di altro ente pubblico, o dell'Unione europea o col pretesto di far esonerare un individuo dal servizio militare, nonché il soggetto che commette tale frode abusando della qualità di operatore del sistema. Tale ultima ipotesi trova la sua *ratio* nell'agevolazione alla commissione del reato derivante dalla posizione di privilegio ricoperta dal soggetto attivo, nonché dalla maggiore pericolosità della condotta [347]. In tal caso, infatti, la frode appare più grave in ragione della violazione dell'obbligo di fedeltà verso il titolare o l'utente del sistema informatico, nonché nei confronti dei soggetti i cui interessi economici sono gestiti dal sistema: si ravvisano maggiori

[344] Sul punto v. *supra* § 2.2.4.

[345] In argomento v. PECORELLA, *Truffe* on-line, cit.

[346] Sul punto v. CAMPEIS, *La frode informatica,* cit., 921.

[347] *Ibidem*; inoltre, cfr. CUOMO, RAZZANTE, *La nuova disciplina dei reati informatici,* cit., 167: «la qualità di "operatore del sistema "non è richiesta per la commissione dell'azione, ma costituisce una circostanza aggravante, per la particolare posizione dell'agente che ha maggiore occasione di influire sull' intero processo di elaborazione, trattamento e diffusione dei dati».

occasioni di intervenire abusivamente sui dati e programmi, causando una notevole vulnerabilità degli stessi, oltreché un maggiore disvalore dell'offesa arrecata.

Si discute se debba considerarsi "operatore del sistema" solo il tecnico informatico che abbia il controllo delle fasi di elaborazione di ciascun dato, precludendo, quindi, tale qualifica al semplice operatore con funzioni esecutive e manuali, oppure se possa ritenersi tale ogni tecnico legittimato ad agire sul computer.

Sembra doversi considerare "operatore del sistema" qualunque soggetto che possa legittimamente mettersi in contatto con il sistema stesso, in virtù della qualificazione professionale o delle conoscenze aggiuntive e specifiche rispetto a quelle di un qualunque operatore del sistema[348].

Il d.l. n. 93/2013 ha introdotto al terzo comma del presente articolo una nuova circostanza aggravante ad effetto speciale, che sanziona più gravemente il soggetto che commette il reato di frode informatica con furto o indebito utilizzo di identità digitale in danno di uno o più individui.

Innanzitutto, è stata posta la questione inerente alla possibilità di configurare la suddetta previsione come una fattispecie autonoma e non come una circostanza aggravante del reato di cui all'art. 640-*ter* c.p., ma sia la dottrina maggioritaria che la giurisprudenza si sono espresse a favore della seconda soluzione.

L'espresso riferimento al "furto" non può ricondursi all'art. 624 c.p., essendo l'"identità" un'entità immateriale, e come tale non assoggettabile ad impossessamento. In tal modo sembra che il legislatore abbia voluto "materializzare" l'identità personale attraverso cui ciascun soggetto si proietta nel *web*.

Con la locuzione "furto d' identità" egli ha presumibilmente voluto riferirsi alla definizione data dall'art. 30-*bis* del d.lgs. n. 141/2010, secondo cui «per furto d'identità si deve intendere: l'impersonificazione totale, mediante occultamento della propria identità attraverso l'uso indebito di dati relativi all'identità e al reddito

[348] V. CAMPEIS, *La frode informatica*, cit.,921; v, anche MINICUCCI, *Le frodi informatiche*, cit., 838 che richiama Cass. pen., 11 novembre 2009, n. 44720, in *C.E.D. Cass*., rv. 245696: «la giurisprudenza ha qualificato "operatore del sistema" colui il quale, in qualità di operatore, programmatore o analista, deve necessariamente avvalersi del sistema informatico per espletare le mansioni del suo ufficio, utilizzandolo per una finalità diversa da quella legittimante, valorizzando così la relazione fiduciaria che lo lega al titolare del sistema violato».

di un altro soggetto, in vita o deceduto; l'impersonificazione parziale, la quale avviene tramite l'impiego, in forma combinata, di dati relativi alla propria persona e l'uso indebito di dati relativi ad un altro soggetto»[349].

Alla luce di tale riferimento normativo sembrerebbe che l'indebito utilizzo sia strumentale al furto d'identità digitale, e non una condotta alternativa, come invece potrebbe emergere dalla lettura del terzo comma, in ragione della disgiunzione "o" utilizzata dal legislatore.

Sembra corretto affermare che tra il furto di identità digitale e l'indebito utilizzo di dati altrui vi sia un rapporto di mezzo a fine, poiché il primo si riferisce alla captazione abusiva, mentre il secondo riguarda un impiego non autorizzato, realizzabile anche senza furto[350].

La suddetta circostanza, con riguardo agli effetti, si sostanzia in una sostituzione di persona che in caso di furto di identità digitale si realizza attraverso un'apprensione illecita dei dati personali, mentre nel caso di indebito utilizzo mediante un uso distorto di dati regolarmente ottenuti.

Nella maggior parte dei casi, la circostanza di cui al comma 3 dell'art. 640-*ter* c.p. è volta a colpire le frodi informatiche realizzate attraverso il *phishing*, sfruttando le altrui credenziali fraudolentemente ottenute[351].

È opportuno aggiungere, per completezza, che tra i reati presupposto della responsabilità amministrativa dipendente da reato delle persone giuridiche, secondo quanto disposto dall'art. 24 del d.lgs. 231/2001[352], figura anche il delitto di frode

---

[349] V. MINICUCCI, *Le frodi informatiche,* cit., 839.

[350] In argomento *ivi*, 840: «peraltro, l'uso dei dati non deve necessariamente riverberarsi in danno della persona offesa dall' evento tipico della frode informatica, posto che la condotta del comma 3 può essere commessa in danno di uno o più soggetti, con parallela riduzione dell'ambito applicativo della truffa semplice in ambito informatico».

[351] *Ivi*, 839, s.: «in questo senso v'è anche chi ha ipotizzato che la fattispecie aggravata finisca con l'assorbire il reato di sostituzione di persona *ex* art. 494 c.p. eventualmente integrato nel caso di specie».

[352] Art. 24 del D.lgs. 231/2001: «Indebita percezione di erogazioni, truffa in danno dello Stato o di un ente pubblico o per il conseguimento di erogazioni pubbliche e frode informatica in danno dello Stato o di un ente pubblico. In relazione alla commissione dei delitti di cui agli articoli 316 bis, 316 ter, 640 comma 2 n.1, 640 bis e 640 ter se commesso in danno dello Stato o di altro ente pubblico, del codice penale, si applica all'ente la sanzione pecuniaria fino a cinquecento quote. Se, in seguito alla commissione dei delitti di cui al comma 1, l'ente ha conseguito un profitto di rilevante entità o è derivato un danno di particolare gravità, si applica la sanzione pecuniaria da duecento a seicento quote. Nei casi previsti dai commi precedenti, si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c), d) ed e)».

informatica, la quale rileva se commessa in danno dello Stato o di altro ente pubblico.

2.3.1 La frode informatica e i rapporti con le altre figure delittuose

La frode informatica è una figura *criminis* che si può porre in rapporto con altre figure di reato, tra le quali, in particolare, la truffa *ex* art. 640 c.p., la frode informatica del soggetto che presta servizi di certificazione di firma elettronica *ex* art. 640-*quinquies*, l'accesso abusivo ad un sistema informatico o telematico *ex* art. 615-*ter*, il danneggiamento di sistemi informatici o telematici *ex* art. 635-*bis*, e l'indebito utilizzo e falsificazione di carte di credito e di pagamento *ex* art. 493-*ter* c.p.

Innanzitutto, è opportuno definire le analogie e le differenze esistenti tra il delitto di frode informatica e quello di truffa *ex* art. 640 c.p., al fine di poter precisare la natura del rapporto intercorrente tra i due.

Il reato di truffa si fonda su una relazione intersoggettiva tra persone fisiche, in cui il soggetto attivo, al fine di ottenere un profitto, inganna, mediante artifici o raggiri, il soggetto passivo, inducendolo a compiere un atto di disposizione patrimoniale: si tratta dunque di un reato a cooperazione artificiosa con la vittima. Inoltre, come già detto in precedenza, si tratta di un delitto a forma vincolata, poiché la condotta ingannatoria deve necessariamente essere realizzata mediante artifici o raggiri rivolti ad indurre in errore una persona fisica, che è così spinta ad autodanneggiarsi.

Al contrario, nella frode informatica[353] si realizza un ingiusto profitto con altrui danno per effetto dell'alterazione del funzionamento del sistema in qualsiasi modo, o dell'intrusione abusiva con qualsiasi modalità su dati informazioni o programmi: si tratta di un reato a forma libera in cui non compare alcun riferimento agli artifici o raggiri volti ad influenzare la volontà del soggetto passivo, del quale non è richiesta né la collaborazione, né la disposizione di un atto patrimoniale; la condotta fraudolenta, libera, è rivolta direttamente al sistema informatico o

[353] V. SCOPINARO, *Internet e reati contro il patrimonio*, cit., 41.: la frode informatica viene definita fattispecie di aggressione unilaterale.

telematico. Nella frode informatica, quindi, si agisce direttamente sullo strumento elettronico, causando così un ingiusto profitto con altrui danno.

Ad ogni modo, sebbene siano innegabili le differenze suesposte, le due fattispecie di reato presentano alcuni elementi comuni, ragion per cui alcuni hanno sostenuto la tesi, non condivisibile, secondo cui la frode informatica avrebbe rimodellato la struttura tradizionale del reato di truffa[354].

Entrambi i delitti sono posti a tutela del patrimonio, e in ambedue i casi si tratta di reato a doppio evento, il cui momento consumativo è quello dell'effettivo conseguimento dell'ingiusto profitto da parte dell'agente o di un terzo, con relativo danno patrimoniale nei confronti dell'offeso; inoltre, sia nella frode informatica che nella truffa l'elemento soggettivo richiesto è il dolo generico.

Secondo un determinato orientamento, la norma di cui all'art. 640-*ter* c.p. rappresenterebbe un'ipotesi di delitto speciale rispetto alla truffa[355], ma, come già precedentemente affermato, tale opinione non sembra potersi condividere, in ragione della presenza di elementi diversi che determinano l'autonomia strutturale del reato di frode informatica, escludendo così la possibilità di ravvisare un qualunque rapporto di specialità tra le due fattispecie criminose[356].

Dunque, occorre distinguere i fatti connessi all'informatica in cui vi è induzione in errore di un soggetto da quelli in cui si verifica un'alterazione o un intervento abusivo sul sistema informatico, poiché nel primo caso ricorre il reato di cui all'art. 640 c.p., mentre nel secondo quello di cui all'art. 640-*ter* c.p.

Il delitto di frode informatica del soggetto che presta servizi di certificazione di firma elettronica è stato introdotto nel codice penale, all'art. 640-*quinquies*, dall'art. 5 della Legge n. 48/2008.

Tale norma punisce il soggetto che, prestando servizi di certificazione di firma elettronica, al fine di procurare un ingiusto vantaggio a sé o ad altri ovvero al fine

---

[354] Sul punto v. CUOMO, RAZZANTE, *La nuova disciplina dei reati informatici*, cit., 163; PARODI, *La frode informatica: presente e futuro delle applicazioni criminali nell' uso dei* software, in Criminalità informatica, a cura di Sarzana di Sant'Ippolito, in *Dir. pen. proc.*, 1997, 12, 1538; per contro v. MINICUCCI, *Le frodi informatiche*, cit., 828 e CAMPEIS, *La frode informatica*, cit., 919 che afferma che la frode informatica solo apparentemente riproduce lo schema del reato di truffa.

[355] V. PICA, *Diritto penale delle tecnologie informatiche*, 1999, Torino, 141 e 162; v. anche CUOMO, RAZZANTE, *La nuova disciplina dei reati informatici*, cit., 163 e 167, secondo cui «la specificità del reato di frode informatica rispetto a quello di truffa esclude la possibilità di concorso formale tra le due fattispecie».

[356] V. FANELLI, *Telefonate abusive e frode informatica*, in *Foro it.*, 1999, 610.

di provocare un altrui danno, contravviene agli obblighi stabiliti dalla legge per il rilascio di un certificato qualificato[357].

Sebbene la rubrica della norma parli di frode informatica commessa da un soggetto qualificato, ovverosia il certificatore, in tale ipotesi non si ravvisa alcuna alterazione di funzionamento del sistema, né tantomeno un'intromissione abusiva, essendo richiesta, al contrario, la mera violazione degli obblighi di legge per il rilascio del certificato. Dunque, a differenza della fattispecie di cui all'art. 640-*ter*, la norma in esame non prevede alcun requisito di fraudolenza, ed è volta a sanzionare la maggiore offensivista della condotta posta in essere dal certificatore per la violazione degli obblighi stabiliti dall'art. 32 del d.lgs. 82/2005, anche detto "Codice dell'amministrazione digitale"[358].

Non di rado l'azione fraudolenta di cui all'art. 640-*ter* viene posta in essere unitamente al delitto di accesso abusivo ad un sistema informatico o telematico *ex* art. 615-*ter* c.p., prodromico alla commissione della frode informatica. In tali casi, infatti, l'accesso abusivo non è fine a sé stesso ma è funzionale alla commissione della frode informatica. È dunque ammesso il concorso del reato in esame con quello di cui all'art. 615-*ter*, in ragione delle differenti condotte sanzionate e della diversità dei beni giuridici tutelati: l'accesso abusivo ad un sistema informatico o telematico è posto a salvaguardia del domicilio informatico sia sotto il profilo dello *ius excludendi alios*, sia con riguardo alle modalità di accesso di soggetti autorizzati; la frode informatica, invece, tutela il patrimonio punendo la condotta di alterazione o intervento senza diritto sul sistema informatico al fine di conseguire un profitto con altrui danno[359]. Inoltre, il delitto di accesso abusivo può essere commesso solo con riferimento ai sistemi protetti, condizione non richiesta per la realizzazione della frode informatica, la quale, diversamente dal delitto di cui all'art.615-*ter*, richiede obbligatoriamente, ai fini della consumazione, la manipolazione del sistema informatico o l'intervento senza diritto sui dati, volti a conseguire profitto con altrui danno[360].

---

[357] V. CAMPEIS, *La frode informatica*, cit., 921.

[358] V. CUOMO, RAZZANTE, *La nuova disciplina dei reati informatici*, cit., 172 s.

[359] In argomento v. Cass. pen, Sez.II, 29 maggio 2019, n. 26604, in *C.E.D. Cass.*, rv. 276427.

[360] Sul punto v. AMATO, DESTITO, DEZZANI, SANTORIELLO, *I reati informatici*, cit., 113 s.

Nel caso in cui si volesse considerare la condotta di violazione delle misure di protezione prodromica alla realizzazione della frode informatica ricompresa in quella contemplata dal reato di cui all'art. 640-*ter* c.p., come se si trattasse di un antefatto non punibile, si rischierebbe di sanzionare in egual modo un soggetto che per commettere la frode abbia posto in essere anche un accesso abusivo e uno che abbia realizzato la condotta fraudolenta senza violare alcuna protezione[361].

Il reato di danneggiamento di informazioni, dati e programmi informatici di cui all'art. 635-*bis* c.p.[362] assume natura residuale rispetto al reato di frode informatica, poiché il testo della norma contempla la clausola "salvo che il fatto costituisca più grave reato"; pertanto, ogniqualvolta sia conseguito un ingiusto profitto con altrui danno – elemento non richiesto dal delitto di cui all'art. 635-*bis* – da una condotta di distruzione, deterioramento, cancellazione, alterazione o soppressione di informazioni, dati o programmi informatici altrui si deve ritenere applicabile il reato di cui all'art. 640-*ter*, poiché punito più severamente[363].

Infine, integra il reato di cui all'art 493-*ter* c.p.[364], e non quello di frode informatica, la condotta di indebito utilizzo di carta di credito, quale mezzo di pagamento o prelievo, in caso di assenza di alterazione o intervento sul sistema informatico o telematico, anche in virtù del fatto che il bene giuridico, in tal caso, assume connotazioni pubblicistiche riferibili alla fede pubblica[365].

---

[361] *Ivi*, 114.

[362] Art. 635-*bis* c.p.: «Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre anni. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni».

[363] Sul punto v. MASI, *Frodi informatiche e attività bancarie*, in *Riv. pen. econ*., 1995, 4, 430; secondo quanto sostenuto da AMATO, DESTITO, DEZZANI, SANTORIELLO, *I reati informatici*, cit., 114 s.: «laddove l'intervento manipolatorio abbia finito con il pregiudicare la funzionalità del sistema, danneggiandolo, oltre alla frode informatica sarà ravvisabile il reato di danneggiamento di sistemi informatici o telematici».

[364] Art. 493-*ter* c.p. comma primo: «chiunque al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, è punito con la reclusione da uno a cinque anni e con la multa da 310 euro a 1.550 euro. Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per altri, falsifica o altera carte di credito o di pagamento o qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, ovvero possiede, cede o acquisisce tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi».

[365] MINICUCCI, *Le frodi informatiche*, cit., 844: «In giurisprudenza, tuttavia, è ancora presente un solido orientamento che ritiene integrato il delitto dell'art. 640-*ter* nel caso in cui l'agente, servendosi di una carta di credito falsificata e di un codice di accesso fraudolentemente

captato, penetri abusivamente nel sistema informatico bancario ed effettui illecite operazioni di trasferimento fondi, tra cui quella di prelievo di contanti attraverso i servizi di cassa continua[…]».

CAPITOLO III

IL PHISHING ATTACK

3.1 Introduzione del fenomeno di *social engineering*. Le fasi del *phishing.*

Nel contesto della criminalità digitale, e più precisamente nell' ambito delle truffe *on-line*, assume particolare rilievo il *phishing*[366], quale fenomeno straordinariamente dinamico ed in costante evoluzione.

Più esattamente, si tratta di un'articolata tecnica fraudolenta di *social engineering*[367] diretta a carpire dati e informazioni personali di un soggetto, mediante condotte ingannevoli, al fine di realizzare nel *cyberspace*, quale ambiente prediletto per la sua manifestazione e diffusione, furti di identità digitale e un uso inappropriato e senza diritto delle informazioni stesse[368]. L*'iter criminis*, infatti, prevede una prima raccolta dei dati della vittima, alla quale segue un'ulteriore condotta realizzata totalmente *on-line*.

L'origine etimologica del termine "*phishing*" sembrerebbe essere incerta, presumibilmente derivante dal connubio delle parole "*harvesting*" e "*password*" – traducibili con "raccolta di password" –, o "*password*" e "*fishing*" – vale a dire "pesca di password", ovvero "*fishing*" e "*phreaking*" – riferite all' uso di frequenze per manipolare un sistema telefonico[369].

L'intento del *phisher* è quello di indurre l'utente a fornire i suoi dati personali, relativi alle credenziali di accesso a conti correnti o servizi bancari telematici, ai numeri di carte di credito o di pagamento, a *username* e *password* per introdursi in aree riservate di siti di diverso tipo, al numero del conto corrente stesso,

---

[366] V. TRUNFIO, CRISAFI, *Il* phishing, in CENDON (diretto da), *Trattato dei nuovi danni, informazioni erronee, soggetti deboli, illeciti informatici, danni ambientali*, Vol. V, Padova, 2011, 959: si tratta di un fenomeno decisamente complesso e strutturato di cui non è data una definizione in alcuna norma dell'ordinamento giuridico italiano; ha iniziato ad emergere intorno alla metà degli anni '90, e attualmente rappresenta un effettivo allarme per la sicurezza informatica e dei servizi finanziari, nonché per la tutela dei consumatori stessi, essendosi nel corso degli anni sempre più rafforzato, ricorrendo altresì all'uso di tecniche sempre più sofisticate.

[367] Le tecniche di ingegneria sociale si fondano su abilità di natura psicologica e sociale, e sono volte a manipolare la mente umana per ottenere le informazioni sensibili degli utenti: per approfondire sul punto v. *supra* §1.2.1.

[368] Cfr. FLOR, Phishing, identity theft *e* identity abuse. *Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. proc. pen*., 2007, 2-3, 902 s.

[369] *Ivi*, 903.

ai riferimenti della carta di identità o di altro documento identificativo, al fine di utilizzare gli stessi dati ottenuti per accedere a servizi riservati *on-line*, assumendo l'identità digitale della vittima[370].

Il conseguimento del suindicato obiettivo dipende principalmente dalla capacità persuasiva del *phisher* e dalle sue abilità tecnico-informatiche, nonché dalle reali opportunità e utilità offerte dalla Rete[371].

Normalmente, il fenomeno si manifesta per mezzo dell'invio di messaggi di posta elettronica, apparentemente provenienti da enti o istituzioni reali, recanti immagini o informazioni specificatamente elaborati per influenzare psicologicamente la vittima e per trarla in inganno. Le "*e-mail* esca" sono indirizzate ad un considerevole numero di utenti sconosciuti, i quali sono indotti a collegarsi a siti *web* fittizi, sebbene a prima vista possano apparire autentici, e sono incoraggiati ad inserire le proprie credenziali di accesso ad aree strettamente riservate su *form o link* appositamente predisposti dal *phisher*[372].

Generalmente, infatti, i messaggi ingannevoli in questione hanno ad oggetto notizie preoccupanti relative a possibili problemi tecnici o ad accessi sospetti, con la finalità di convincere l'utente a cliccare sui *link* indicati, graficamente identici a quelli originali, e ad immettere le informazioni sensibili richieste per risolvere le suddette criticità.

Lo scopo dell'attaccante di carpire le suddette informazioni si realizza nel momento in cui la vittima fornisce effettivamente e volontariamente[373] i dati, ovvero nel caso in cui questi siano prelevati autonomamente mediante programmi *keylogger* o *web trojan*, autoinstallanti[374], ovvero scaricati tramite la navigazione o su sollecitazione della *mail*.

---

[370] *Ibidem*.

[371] *Ivi*, 904.

[372] V. CAJANI, COSTABILE, MAZZARACO, Phishing *e furto d'identità digitale: indagini informatiche e sicurezza bancaria*, Milano, 2008, 14 s.; v. anche cfr. FLOR, Phishing, identity theft *e* identity abuse, cit., 904: «oltre a queste forme "pure" di *phishing* se ne sono sviluppate di "miste", connotate dalla necessaria presenza di un soggetto diverso dal *phisher*, per le quali sorge il problema di determinare la concreta rilevanza giuridica, in base al contributo – concorsuale o non concorsuale – nella commissione di un illecito penale».

[373] Cfr. CAJANI, COSTABILE, MAZZARACO, Phishing *e furto d'identità digitale,* cit.,14.

[374] MINICUCCI, *Le frodi informatiche*, in CADOPPI, CANESTRARI, MANNA, PAPA (diretto da), Cybercrime, Torino, 2019, 842.

Nel corso degli anni tale fenomeno si è costantemente evoluto ed affinato, e il numero dei *phishing attacks* si è moltiplicato; sono state sviluppate, infatti, ulteriori tecniche di attacco, più subdole, basate sull'impiego di *software malware*, quali *trojan o spyware*[375]. Tuttavia, non sembra possibile determinare con certezza la reale dimensione del fenomeno del *phishing*, poiché si ravvisa un elevata "cifra oscura" di casi non denunciati, i quali, di conseguenza, non vengono segnalati nei numerosi e specifici rapporti periodici, che comunque evidenziano una costante crescita complessiva del detto fenomeno fraudolento[376].

Il *phisher* sceglie di attaccare singolarmente gli individui e non un sistema centrale contenente le informazioni sensibili di migliaia di utenti, poiché è molto più semplice aggredire un singolo che non possiede né le capacità per riconoscere gli attacchi né le più basilari tecnologie di difesa per proteggersi, piuttosto che una struttura organizzata e dotata di misure di sicurezza a più livelli.

Solitamente il *phishing attack* prevede sei diverse fasi: nella prima fase, denominata "*planning*", il *phisher* individua la vittima, l'oggetto da rubare, quali tecniche usare e quali obiettivi perseguire con tale frode; la seconda è quella di "*setup*" in cui l'attaccante organizza l'attacco, predisponendo i *tools* e i relativi meccanismi funzionali a realizzarlo, procurandosi inoltre i contatti delle potenziali vittime; nella terza fase, chiamata "*attack*", il *phisher* inizia ad instaurare un contatto con l' utente servendosi di strumenti e opportunità offerti dalla Rete, quali ad esempio, *email, chat,* siti *web e malware*, con lo scopo di indurre la vittima a porre in essere azioni che gli consentano di scoprire le sue credenziali; è nella quarta fase, indicata con il termine "*collection*", che il *phisher* sottrae effettivamente le credenziali degli utenti attraverso *web form, email,* telefono e *malware*; la quinta fase è definita "*fraud*" e si riferisce all' utilizzo delle credenziali raccolte da parte

[375] Sul punto v. CAJANI, COSTABILE, MAZZARACO, *Phishing e furto d'identità digitale*, cit.,14; Il *phishing* realizzato tramite *malware* implica l'esecuzione di un s*oftware* malevolo sul computer della vittima, che può essere divulgato approfittando dei *bug* del sistema di protezione o impiegando tecniche di ingegneria sociale. Come evidenziato nel Rapporto Clusit 2020 gli attacchi mirati, c.d. *"whaling" o "spear phishing*", in cui l'attaccante finge di essere un manager d' azienda e incita un dipendente della stessa ad eseguire un pagamento a suo favore, sono in forte crescita.

[376] Sul punto cfr. FLOR, Phishing, identity theft *e* identity abuse, cit., 904 s.: l'andamento generale del fenomeno del *phishing* può altresì dedursi dall'analisi e dai rapporti redatti dall'*Anti-Phishing Working Group,* che «è un'associazione globale pan-industriale e di *law enforcement* il cui obiettivo primario è il contrasto alle frodi e ai furti di identità realizzati attraverso il *phishing, il pharming e l'email spoofing*».

del *phisher*, il quale le commercia, vende o impiega per altri scopi fraudolenti – infatti le suddette credenziali possono essere sfruttate per acquistare beni, rubare denaro dal conto corrente dell'utente, per furto d'identità o per ricavare informazioni per fingersi la vittima o addirittura per riciclare denaro –; la sesta ed ultima fase è indicata come "*post attack*", ed è quella in cui il *phisher*, realizzato il suo obiettivo, interrompe i meccanismi, nasconde le tracce, verifica che l'attacco sia andato a buon fine, osserva le reazioni e pianifica nuovi attacchi[377].

3.1.1 Le principali tipologie di *phishing.*

Il *phishing*, quale fenomeno fraudolento volto ad ottenere i dati sensibili delle vittime e ad utilizzare gli stessi per ulteriori scopi illeciti, può realizzarsi attraverso diversi tipi di attacchi, tra i quali i più importanti sono quelli di seguito riportati; in ciascuna tipologia si possono ravvisare le suindicate sei fasi distintive del *phishing*.

Il "*deceptive phishing*" – tradotto come "*phishing* ingannevole"– rappresenta la tipologia di attacco più comune, e consiste nell'invio di numerose *e-mail* ingannevoli ad un elevato numero di destinatari, quali potenziali vittime del messaggio di posta elettronica, contenente l'invito a cliccare su un *link* appositamente indicato e ad inserire le proprie credenziali sul sito *web* fraudolento a cui viene indirizzato, affinché il *phisher* possa conoscere i dati sensibili riservati aggiunti da ciascun utente, e successivamente riutilizzarli per fingersi la vittima, trasferire denaro da un conto all'altro, acquistare merci o causare altro tipo di danno. Non di rado l'attaccante, anziché causare direttamente il danno economico, rivende le informazioni illegalmente carpite su un mercato secondario mediante *forum on-line* e canali *chat*[378].

Si ravvisano non poche variazioni negli schemi di *phishing* fondati sull' inganno: infatti, in alcuni casi il testo del messaggio può contenere direttamente la riproduzione di una pagina di *login*, senza la necessità di dover attivare il *browser* mediante *click* sul collegamento *web*, oppure in altri casi può essere riportato un indirizzo *IP* numerico al posto del nome dell'*host* nella stringa di connessione ad

[377] V. CAJANI, COSTABILE, MAZZARACO, *Phishing e furto d'identità digitale*, cit.,15 s.
[378] *Ivi*, 16 s.

un sito fittizio di *phishing*; quindi si può ingannare la vittima in qualunque modo lasciandole credere che sta comunicando con un sito legittimo[379].

Le *e-mail* di *phishing*, inizialmente scritte in inglese o in italiano scorretto, nella gran parte dei casi sono solite simulare l'impostazione grafica, il tenore linguistico e il contenuto di una reale comunicazione di un ente, come ad esempio un istituto bancario. Tuttavia, il *link* indicato nel testo del messaggio riporta ad una pagina *web* che solo apparentemente sembra essere quella del suddetto ente, ma che in realtà è creata *ad hoc* dal *phisher* per sottrarre e memorizzare le informazioni riservate fornite dagli utenti inconsapevoli[380].

Ad ogni modo, è bene precisare che negli ultimi anni si è manifestata la c.d. "tencica di *hijacking*", per cui le *e-mail* di *phishing* sono state sempre più spesso sostituite da *malware* volti a carpire informazioni sensibili sui conti correnti bancari o a indirizzare gli utenti a siti clone[381].

Ulteriore tipologia di attacco è quella del *phishing* basato su *malware*, il quale implica l'esecuzione di un *software* malevolo, diffuso sia tramite inganni di *social engineering* sia approfittando dei punti deboli del sistema di protezione di cui è dotato il computer della vittima ignara.

Un classico inganno di ingegneria sociale consiste nell'indurre un soggetto ad aprire l'allegato di una *e-mail* o a scaricare un documento da un determinato sito *web* contenente il codice maligno. La divulgazione del suddetto codice può avvenire mediante attacchi alla sicurezza, ovverosia tramite la diffusione di *worm* o *virus* che sfruttano le debolezze del sistema per installare il codice malevolo, o mettendo a disposizione il codice su un sito *web* che approfitta di una carenza di sicurezza.

---

[379] *Ivi*, 17.

[380] *Ivi*, 24, ove si sottolinea che nella gran parte dei casi gli utenti sono soliti ricevere *e-mail* di questo tipo: «*e-mail* che invita ad accedere al sito della banca per ottenere il nuovo pin di sicurezza; *e-mail* contenente un avviso di addebito in conto di un importo non indifferente […]: maggiori dettagli il destinatario li può trovare nel sito indicato nella *e-mail*, per accedere al quale viene poi richiesta la *user-id* e la *password*, in modo da poterla catturare; *e-mail* che invita ad accedere al sito della banca proprio perché fantomatici *phishers* avrebbero attentato alla sicurezza del conto corrente del cliente: il destinatario, accedendo al sito riceve sul computer un programma *trojan* che si metterà "in ascolto" e provvederà a raccogliere i dati digitati dal cliente sul suo personal computer e, successivamente, ad inviarli all' *hacker* o ad una banda criminale».

[381] *Ivi*, 24 s.

Inoltre, la navigazione su Internet può essere reindirizzata su una pagina *web* fraudolenta utilizzando tecniche di ingegneria sociale, come avviene quando si utilizzano i messaggi *spam* o immettendo un contenuto maligno in un sito *web* legittimo, approfittando delle vulnerabilità del *web server*[382].

Questa tipologia di *phishing* basato su *malware* può, a sua volta, assumere diverse forme[383]: la prima è quella dei "*keylogger*" – c.d. "registratori di tasti" – , ovverosia programmi autoinstallanti nel *browser web* e nel *driver* dello strumento di *input*, al fine di controllare i dati inseriti ed inviare quelli utili ad un *server* di *phishing*; la seconda è quella della "*session hijacking*" – c.d. "dirottatori di sistema" – , attacco con cui vengono tracciate le attività in rete di un soggetto per mezzo di un elemento non legittimo del *browser*, e non appena l'utente immette le proprie credenziali, il *software* "devia" la sessione per compiere le azioni finalizzate a frodare la vittima; altra forma è quella dei "*web trojans*" – intesi come cavalli di troia in rete –, vale a dire programmi funzionali ad agganciarsi alle "finestre di *login*" per sottrarre le credenziali agli utenti che credono di inserirle su un sito *web* legittimo, ma in realtà sono indirizzate all'attaccante per l'utilizzo fraudolento; ulteriore forma è quella degli "attacchi di riconfigurazione del sistema", i quali correggono le impostazioni sul computer di un soggetto causando la compromissione dei dati[384].

Il codice maligno, una volta eseguito sul computer della vittima, è capace di sottrarre direttamente le informazioni riservate in esso memorizzate; tali informazioni sono relative a *password,* codici di attivazione di *software, e-mail* strettamente personali, numeri di carte di credito e altri tipi di dati memorizzati sul computer dell'utente.

Una particolare metodologia è quella del *phishing* con inserimento, in un sito legittimo, di contenuti malevoli, i quali possono reindirizzare ad altre pagine

[382] *Ivi*, 26.

[383] Per approfondire sul punto v. CAPONE, *Le principali tipologie di "*phishing attac*k"*, in *www.cyberlaws.it*, 27 giugno 2018.

[384] Cfr. CAJANI, COSTABILE, MAZZARACO, Phishing *e furto d'identità digitale*, cit., 28: «Un tipo di attacco di configurazione del sistema consiste nel modificare i *server DNS* dell'utente, dirottando così la sua navigazione su *Internet* verso siti fraudolenti. Un altro tipo di attacco di riconfigurazione di sistema consiste nell'installare un *proxy web* attraverso il quale transita il traffico dell'utente».

web, inserire un *malware* sul computer della vittima o immettere un *frame* di contenuti che può dirottare i dati verso un *server di phishing*.

Il *phishing "man in the middl*e" è una tipologia di attacco con il quale il *phisher* si interpone tra la vittima e il sito legittimo: «i messaggi destinati al sito legittimo vengono in realtà passati al *phisher* il quale salva le informazioni di interesse, inoltra i messaggi al sito legittimo e inoltra all' utente le risposte di ritorno»[385].

Si tratta di attacchi che possono essere impiegati anche per la deviazione delle sessioni, con o senza la memorizzazione delle informazioni pregiudicate.

È molto difficile che l'utente si accorga di questa forma di attacco, poiché il sito sembra funzionare correttamente e potrebbe non esservi alcuna traccia esterna sospetta.

Generalmente il traffico *Secure Socket Layer* in rete – protocollo s*tandard* che assicura la protezione durante il passaggio di dati da un *browser* ad un s*erver web* – non sembra esposto a questo tipo di attacco, poiché la fase di "*handshake*" impiegata dal *SSL* consente che la sessione sia attivata con la parte il cui nome è precisato nel certificato del *server*, garantendo altresì la riservatezza della chiave di sessione, la quale è funzionale a criptare il traffico *SSL* che potrà essere decifrato solo per mezzo di un intercettatore. Ciononostante, un "*man in the middle*" può elaborare i suoi certificati per un sito assicurato con *SSL*, decriptare il traffico, prelevare le informazioni riservate di interesse, e cifrare ancora una volta il traffico per comunicare con l'altra parte[386].

Un'altra forma di *phishing* è quella che si basa sui motori di ricerca, in cui il *phisher* predispone siti *web* che pubblicizzano a prezzi estremamente convenienti finti prodotti, ottiene l'indicizzazione delle stesse sui motori di ricerca e attende che gli utenti immettano le proprie credenziali o informazioni riservate per completare un ordine, una registrazione o un pagamento, per poi sottrarle[387].

---

[385] Cfr. CAJANI, COSTABILE, MAZZARACO, Phishing *e furto d'identità digitale*, cit., 29.

[386] Sul punto *ivi*, 29 s.

[387] Cfr. CAJANI, COSTABILE, MAZZARACO, Phishing *e furto d'identità digitale*, cit., 30: «In particolare sono stati utilizzati con successo siti *web* di banche fraudolente: in questo caso, il *phisher* crea una pagina di pubblicità per un conto corrente con tasso di interesse leggermente più alto di una qualunque vera banca. Le vittime trovano la banca attraverso i motori di ricerca e inseriscono le credenziali del loro conto bancario per un "trasferimento di somme" verso il nuovo "conto"».

Un'altra peculiare tipologia di *phishing* è quella che sfrutta il "*rock phish kit*", ovverosia un *software* disponibile *on-line* che consente di realizzare dei siti clone, molto simili a quelli reali, all'interno dei quali sono presenti dei *form* da compilare, attraverso cui vengono sottratti i dati degli utenti ignari. Il suddetto *kit*, inoltre, consente di creare una *e-mail* per lo *spam* che reindirizza al sito clone, e in aggiunta può elaborare innumerevoli siti clone sul medesimo *server* attraverso i quali attaccare più obiettivi simultaneamente. In tal modo il *server* diviene una vera e propria base da cui far partire numerosi attacchi differenziati, al fine di ottimizzare le probabilità di riuscita prima della bonifica del *server* stesso da parte dei gruppi "*antiphishing*"[388].

La breve panoramica sin qui compiuta dimostra come le tipologie di *phishing*, sebbene condividano il medesimo fine, presentano tra loro un diverso *modus operandi*. Tenendo presente quanto sin'ora esposto, è possibile proseguire con l'inquadramento normativo del fenomeno in questione.

3.2 Inquadramento normativo: le norme applicabili

Nell'ordinamento italiano attualmente non si ravvisa una disciplina giuridica *ad hoc* che consideri unitariamente il fenomeno del *phishing*, esistendo, per contro, differenti norme giuridiche nelle quali poter ricondurre le condotte tipiche poste in essere per realizzare le singole fasi che lo contraddistinguono[389].

Al fine di individuare quali fattispecie incriminatrici vengono in rilievo nell'ambito del fenomeno in questione, sembra opportuno proporre una disamina parallela delle fasi costitutive del *phsihing* e delle norme potenzialmente applicabili.

Tuttavia, è bene premettere che il *phishing attack* non aggredisce direttamente il patrimonio dell'utente, ma manifesta una propria ed autonoma dimensione offensiva, il cui nucleo si concretizza nel "furto di dati personali" – o più generalmente "riservati" – che, a sua volta, si traduce nella realizzazione di una

[388] *Ibidem*: «Praticamente il *phisher* installa un "pacchetto multiplo" contenente i siti clone di entità finanziarie italiane e straniere, clonando loghi, testi, grafica, trasformando il *server* ospite in un arsenale pronto a sferrare l'attacco».

[389] Per approfondire sul punto v. TRUNFIO, CRISAFI, *Il phishing*, cit., 960: gli illeciti associati al fenomeno del *phishing* vanno ricondotti nell'alveo di distinte fattispecie penali esistenti, senza pretesa di esaustività, in ragione della dinamicità di tale fenomeno, nonché della capacità di assumere plurime forme di manifestazione e di mutare continuamente *modus operandi*.

serie di operazioni concernenti l'utilizzo illegittimo dei suddetti dati fraudolentemente raccolti[390].

Dunque, rileva certamente la necessità di proteggere la sfera riservata dell'individuo, e più esattamente il diritto «alla corretta e legittima circolazione dei dati *latu sensu* riservati, al controllo sul loro trattamento, o sulla loro destinazione che, a seguito della evoluzione-rivoluzione tecnica, economica e sociale, "quasi per correlazione necessaria", diviene maggiormente vulnerabile»[391].

Inoltre, sebbene si intenda procedere all'analisi delle prospettive applicative delle norme penali vigenti mantenendo la distinzione in fasi antecedentemente proposta, non si può non rilevare come alcune delle manifestazioni criminose proprie del fenomeno in esame assumano una valenza plurioffensiva, astrattamente riferibile a più fasi[392].

Per quel che concerne le prime fasi, relative alla formazione e all'invio del messaggio di posta elettronica, avente ad oggetto il *link* che reindirizza al sito *web* fittizio, solo apparentemente proveniente dal mittente reale, potrebbe ritenersi integrata la fattispecie di sostituzione di persona *ex* art. 494 c.p.[393].

Più precisamente, potrebbe prospettarsi l'applicazione della suddetta disposizione, in quanto con l'*e-mail* in questione il *phisher* utilizza in rete i dati identificativi di un mittente reale, sostituendo illegittimamente la propria all'altrui persona ovvero attribuendosi un falso nome, stato o qualità a cui la legge riconosce effetti giuridici, inducendo così in errore un elevato numero di utenti, al fine di carpire i dati sensibili e le credenziali di ciascuno di essi, procurando un vantaggio a sé o recando un danno a terzi[394].

---

[390] Cfr. FLOR, Phishing, identity theft *e* identity abuse, cit., 906, secondo cui: «[…]l'attitudine intrinsecamente offensiva del fatto incide sull' interesse sostanziale al controllo di dati riservati e personali immessi in un sistema di reti telematiche, in cui le " forme di verifica" dell'"identità" o del profilo personale – per lo svolgimento di molteplici operazioni, fra cui quelle bancarie, finanziarie e commerciali – non avvengono (o non avvengono solo) *face to face*, ma tramite l' attribuzione di " privilegi" abilitativi di natura logica all' accesso a tali sistemi».

[391] *Ibidem.*

[392] *Ibidem.*

[393] Articolo 494 c.p.: «Chiunque, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un sanno, induce talune 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».

[394] FLOR, *Phishing, identity theft e identity abuse,* cit., 907; quindi la condotta di colui che, al fine di procurare a sé o ad altri un vantaggio, si attribuisce nell'*account* di posta elettronica gli

Tuttavia, in ragione delle peculiarità proprie del *web*, l'effettiva configurabilità di tale delitto deve essere verificata in concreto, poiché potrebbero ravvisarsi delle asimmetrie rispetto agli elementi tipici del reato[395].

Inoltre, è bene puntualizzare la limitata possibilità di applicazione dell'art. 494 c.p., poiché la figura *criminis* in questione può delinearsi solo se il messaggio di posta elettronica ingannevole contenga riferimenti ad una persona fisica – ad esempio per mezzo della simulazione di un nome o di uno specifico stato o qualità – , e non anche quando le allusioni siano relative a segni distintivi di una società o di une ente , non potendosi, in tal caso, determinare alcuna sostituzione di persona fisica, e di conseguenza il reato di cui all'art. 494 c.p.[396].

Non sembra configurabile il delitto di sostituzione di persona nei casi in cui i dati riservati o le credenziali identificative degli utenti, fraudolentemente carpiti, siano utilizzati su siti *web*, non essendo integrato l'elemento oggettivo del reato, in quanto l'agente non si attribuisce un falso nome, stato o qualità a cui la legge attribuisce effetti giuridici, e dunque «nel caso in esame non viene in considerazione il bene della conoscenza certa della persona o delle sue qualità essenziali e tantomeno avviene una materiale sostituzione della persona»[397]; in tali ipotesi è possibile configurare tutt'al più il reato di accesso abusivo ad un sistema informatico o telematico *ex* art. 615-*ter* c.p. L'impiego *on-line* dei suddetti dati non induce in errore il sistema informatico, che si limita ad eseguire i comandi impartiti dall'utilizzatore del sistema, il quale può essere comparato con il soggetto legittimato in ragione dell'uso delle credenziali autenticative[398].

Quando la condotta volta a carpire i dati riservati e le credenziali viene realizzata per mezzo della divulgazione di un *malware* nel sistema bersaglio potrà

---

estremi identificativi di un altro individuo, provocando un danno a quest'ultimo e traendo in inganno gli utenti del *web*, integra il delitto di sostituzione di persona *ex* art. 494 c.p., sebbene sia perpetrato in rete, come ammesso da Cass. pen. Sez. V, 14.12.2007, n. 46674, in *www.pluris-cedam.utetgiuridica.it.*

[395] Cfr. FLOR, *Phishing, identity theft e identity abuse,* cit., 907: la natura informatica del "profilo personale" ed il suo impiego in rete sottolineano come la potenziale lesione della affidabilità dei rapporti intersoggettivi si realizza con specifiche modalità tecniche relative all'utilizzo della c.d. "identità virtuale", non completamente coincidenti con gli elementi tipici del delitto in esame, il quale «è chiaramente a forma vincolata commissiva e comporta la necessità di "indurre taluno in errore" con le modalità tassativamente previste dalla norma stessa».

[396] Per approfondire sul punto v. FLOR, *Phishing, identity theft e identity abuse,* cit., 907 s.

[397] *Ivi*, 908.

[398] *Ivi*, 909.

applicarsi il reato di diffusione di programmi diretti a danneggiare o interrompere un sistema informatico ai sensi dell'art. 615-*quinquies*, dal momento che il *software* malevolo è finalizzato a reindirizzare l'utente ignaro a siti *web,* apparentemente identici a quelli reali, appositamente predisposti dal *phisher* per sottrargli le informazioni utili, ravvisandosi così l' ipotesi dell' "alterazione del funzionamento" del sistema utilizzato dalla vittima[399].

Come anticipato, il collegamento ipertestuale ingannatorio generalmente contenuto nel messaggio di posta elettronica ricevuto dall'utente rimanda ad un sito-clone elaborato dal *phisher*, esteriormente identico nel formato e nel contenuto al sito reale. Il suddetto sito *web* fittizio provoca una falsa rappresentazione della realtà nella vittima, inducendola ad inserire le proprie credenziali d'accesso nell'apposito *form* e ad effettuare un atto di disposizione patrimoniale causativo di una *deminutio patrimonii*, consentendo all'agente di ottenere i dati riservati e conseguire un ingiusto profitto: si realizza così la struttura tipica della truffa *ex* art. 640 c.p., quale ipotesi di reato astrattamente configurabile in tal caso.

Il reo, tramite l'invio dell'*e-mail*, inganna la vittima facendole credere di interagire con un determinato ente di fiducia – ad esempio un istituto bancario o una società di *e-commerce* –, inducendola ad inserire i propri dati riservati: si ritiene così perfettamente integrato l'elemento modale della condotta del reato di truffa, ossia gli "artifici o raggiri". In ragione della fittizia rappresentazione della realtà prospettata dal *phisher*, l'utente, indotto in errore per effetto dei suddetti artifici o raggiri, pone in essere l'atto di disposizione patrimoniale da cui deriverà il duplice evento dell'ingiusto profitto per l'agente e dell'altrui danno per colui che subisce il deterioramento patrimoniale.

La suddetta disposizione patrimoniale, quale conseguenza dalla condotta ingannatoria del *phisher*, costituisce il requisito tacito della fattispecie *de quo*, indicando chiaramente la natura del reato a cooperazione artificiosa della vittima, poiché l'induzione in errore non può che riferirsi all'utente ingannato[400]; dunque, laddove manchi il suddetto requisito non potrebbe ritenersi integrato il reato di truffa *ex* art. 640 c.p. Inoltre, nei casi in cui l'atto negoziale sia realizzato

[399] Sul punto v. CAJANI, COSTABILE, MAZZARACO, Phishing *e furto d'identità digitale,* cit., 119.

[400] V. FLOR, Phishing, identity theft *e* identity abuse, cit., 916.

autonomamente dall'agente e non dalla vittima, a seguito dell'accesso alle aree riservate di quest'ultima, difetterebbe la necessaria cooperazione del soggetto ingannato, tale da non potersi configurare il reato in esame[401].

Sembrerebbe potersi ammettere il concorso tra le due ipotesi di reato sin qui considerate, vale a dire tra la sostituzione di persona di cui all'art. 494 c.p. e di truffa *ex* art. 640 c.p., poiché si tratta di due norme poste a salvaguardia di differenti beni giuridici[402].

Nondimeno, la condotta dell'agente che, «al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno»[403], indebitamente si procuri i codici di accesso ad un sistema informatico o telematico difeso da misure di sicurezza è astrattamente idonea ad integrare gli estremi dell'art. 615-*quater* c.p., vale a dire del reato di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici[404].

La fase successiva alla fraudolenta acquisizione dei dati riservati riguarda l'utilizzo delle stesse informazioni per accedere abusivamente a servizi *on-line* o ad aree private della vittima.

L'accesso illegittimo, senza diritto, all'*account* dell'utente, eludendo le misure di sicurezza – e più precisamente di autenticazione – approntate per

---

[401] *Ibidem*. Tuttavia, è bene precisare che secondo alcuni il fatto che l'atto di disposizione patrimoniale sia realizzato in autonomia dal *phisher* non escluderebbe la configurabilità del reato di truffa, poiché l'art. 640 c.p. prevede che l'agente debba ottenere un vantaggio patrimoniale per sé o per altri con altrui danno, non richiedendo altresì che la condotta di disposizione patrimoniale sia compiuta dalla vittima e non dall'agente: sul punto v. Trib. Milano 19 ottobre 2008, in *Corr. merito*, 2009, 3, 285 ss., con nota a sentenza di AGNINO, Computer crime *e fattispecie penali tradizionali: quando il* phishing *integra il delitto di truffa*.

[402] Inoltre, a favore dell'ammissibilità del concorso vi è il fatto che tra gli elementi costitutivi del reato di truffa non si ravvisa la sostituzione di persona: v. Trib. Milano 19 ottobre 2008, in *Corr. merito*, 2009, 3, 288., con nota a sentenza di AGNINO, Computer crime *e fattispecie penali tradizionali: quando il* phishing *integra il delitto di truffa*; sul punto v. anche CAJANI, COSTABILE, MAZZARACO, Phishing *e furto d'identità digitale*, cit.,122.

[403] Cfr. art. 615-*quater* c.p.: «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 a un anno e con la multa sino a euro 5.164. La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-*quater*»; sembra opportuno specificare che si tratta di un reato a dolo specifico, per cui non è necessaria la realizzazione oggettiva del fine per la consumazione dello stesso: v. FLOR, Phishing, identity theft *e* identity abuse, cit., 925.

[404] Sul punto v. CAJANI, COSTABILE, MAZZARACO, *Phishing e furto d'identità digitale*, cit., 121.

assicurare la protezione dei dati in esso contenuti, e quindi del diritto del soggetto titolare all'"ingresso" esclusivo, è idoneo a configurare l'ipotesi del reato di accesso abusivo ad un sistema informatico o telematico ai sensi dell'art. 615-*ter* c.p.[405].

Come evidenziato in precedenza, in ragione dell'eterogeneità dei beni giuridici tutelati si considera ammissibile il concorso tra il reato di truffa *ex* art. 640 c.p. e il reato di accesso abusivo ad un sistema informatico o telematico *ex* art. 615-*ter* c.p.[406].

Nel caso in cui dovesse verificarsi l'acquisizione indebita di credenziali e il successivo impiego delle stesse per effettuare un accesso abusivo dovrà ritenersi applicabile solo l'art. 615-*ter*, e non anche l'art. 615-*quater,* non solo in virtù del fatto che l'accesso abusivo ad un sistema informatico o telematico è considerato un reato più grave e posto a tutela del medesimo bene giuridico protetto dal reato minore di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici, ma anche perché la stessa condotta di detenzione e diffusione abusiva *ex* art. 615-*quater* viene valutata come un antefatto non punibile del reato di accesso abusivo[407].

Qualora il *phisher,* dopo aver ottenuto le credenziali d'accesso dell'utente, dovesse utilizzare le stesse nei relativi *account*, alterando il funzionamento del sistema o intervenendo senza diritto e con qualsivoglia modalità su dati, informazioni o programmi in esso presenti, determinando così l'ingiusto profitto

---

[405] Articolo 615-*ter*, comma 1, c.p.: «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»; in argomento v. anche FLOR, *Phishing, identity theft e identity abuse,* cit., 929 ss.: la norma di cui all'art. 615-t*er*, disposta tra i delitti contro l'inviolabilità del domicilio, è costruita sulla falsariga del reato di violazione di domicilio *ex* art. 614 c.p. «I sistemi informatici e telematici sono stati considerati dal legislatore, infatti, un' "espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantita dall'art. 14 della Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali dagli art. 614 e 615 c.p.", costituendo un ambiente in cui si manifesta una forma di estrinsecazione della personalità umana, che va oltre la sfera domestica o il carattere strettamente personale dei dati o delle informazioni archiviate e trattate nel relativo spazio virtuale». Il bene giuridico tutelato da questa norma si ravvisa nella riservatezza informatica, intesa come interesse esclusivo di disporre e controllare l'area informatica riservata e le informazioni ivi contenute, nonché, quindi, nello *jus excludendi alios*, ovverosia nel diritto dell'utente titolare di escludere l'ingresso indesiderato di altri nel suo "spazio" informatico. La violazione dei mezzi di sicurezza predisposti è indicativa della mancanza del consenso espresso o tacito del titolare del sistema all' accesso altrui.

[406] In argomento v. *supra* § 2.2.5.

[407] Sul punto v. CAJANI, COSTABILE, MAZZARACO, Phishing *e furto d'identità digitale*, cit.,122 s; PECORELLA, *Diritto penale dell'informatica. Ristampa con aggiornamento,* Padova, 2006, 374.

con altrui danno, dovrebbe ritenersi integrato il delitto di frode informatica ai sensi dell'art. 640-*ter* c.p.[408]. In tal caso la condotta dell'agente sarebbe rivolta al sistema informatico e non alla vittima, in quanto finalizzata a manipolare il sistema stesso[409].

Come già detto, non sembra potersi ammettere il concorso tra il reato di frode informatica di cui all'art 640-*ter* c.p. e il reato di truffa *ex* art. 640 c.p.[410], mentre deve ritenersi possibile quello tra l'accesso abusivo ad un sistema informatico o telematico e la frode informatica[411].

Ultimamente si sono sviluppate nuove forme di attacco, c.d. "miste", che includono nell'azione criminosa oltre al *phisher* anche ulteriori soggetti. Più precisamente, fuori dai casi in cui si ravvisi il concorso del terzo nel reato, ovvero al di là delle situazioni in cui si tratti del soggetto passivo o del danneggiato del reato stesso, può ritenersi astrattamente configurabile il delitto di riciclaggio *ex* art. 648-*bis* c.p., qualora la condotta del suddetto soggetto terzo, c.d. *financial manager* o prestaconto, appositamente individuato dal *phisher*, consista nell'offrire a quest'ultimo un conto corrente sul quale poter spostare il denaro, ostacolando cosi l'individuazione della provenienza delittuosa[412].

---

[408] Inoltre, è bene precisare che «secondo quanto ribadito dalla Suprema Corte di Cassazione, integra il reato di frode informatica e non quello di indebita utilizzazione di carte di credito, la condotta di colui che, servendosi di una carta di credito falsificata e di un codice d'accesso fraudolentemente captato in precedenza, penetri abusivamente nel sistema informatico altrui effettuando operazioni illecite per trarne profitto per sé o per altri»: cfr. PINO, Phishing- *Cassazione Penale: risponde di frode informatica l'intestatario della carta prepagata utilizzata per attività di* phishing, in *www.filodiritto.it*, 29 novembre 2018, che richiama Cass. pen. sez. II, 24 ottobre 2018, n. 48553.

[409] Ad esempio, potrebbe integrare il reato di frode informatica la condotta del soggetto che effettui abusivamente l'accesso all'a*ccount* dell'utente inerente a servizi bancari telematici, alterando il funzionamento del sistema informatico o intervenendo senza diritto sulle informazioni *ivi* presenti, e ponendo in essere operazioni finanziarie illecite, dipendenti dal sistema stesso; sul punto v. anche Cass. Pen., Sez. II, 13 ottobre 2015 n. 50140, secondo cui: «[...] l'abusivo utilizzo di codici informatici di terzi [...] è idoneo ad integrare la fattispecie di cui all'art. 640-ter c.p. ove quei codici siano utilizzati per intervenire senza diritto su dati, informazioni o programmi contenuti in un sistema informatico o telematico, al fine di procurare a sé od altri un ingiusto profitto»; tuttavia, contrariamente a tale orientamento, in dottrina v. CAJANI, COSTABILE, MAZZARACO, Phishing *e furto d'identità digitale*, cit., 119 s., secondo cui non sarebbe applicabile al *phishing* la norma relativa alla frode informatica, in quanto le condotte di cui all'art. 640-*ter* si ritengono, in tal caso, insussistenti.

[410] Per approfondire sul punto si rinvia a quanto già detto *supra* § 2.3.1.

[411] Per approfondire sul punto si rinvia a quanto già detto *supra* § 2.3.1.

[412] In argomento v. FLOR, Phishing, identity theft *e* identity abuse, cit., 933 ss.

Per ritenere sussistente il reato in questione il soggetto prestaconto deve aver agito, a fronte di corrispettivo, nonostante la consapevolezza della provenienza illecita delle somme depositate sul conto da lui messo a disposizione. Il *financial manager*, infatti, riceve il denaro, quale conseguenza dell'azione del *phisher* e, al fine impedire la ricostruzione della reale provenienza delle somme, lo trasferisce su un conto appositamente istituito, a seguito del *phishing attack*, facendo ricorso a società di *money transfer*, così da interrompere ogni traccia dei flussi monetari.[413]

Diversamente, può configurarsi il delitto di ricettazione di cui all'art. 648 c.p. nei casi in cui il soggetto prestaconto, cosciente dell'origine criminosa del denaro, abbia percepito le somme senza poi trasferirle sul conto.

Alla luce di quanto detto emerge chiaramente l'esigenza di tenere conto della concreta situazione di riferimento, poiché la condotta del *phisher* può astrattamente configurare i diversi tipi di reati suesposti. Inoltre, per poter inquadrare correttamente il fenomeno è necessario considerare l'evoluzione del *phishing attack*, di cui si dirà di seguito.

3.3 L'evoluzione del fenomeno del *phishing attack*

Il *phishing* è un fenomeno estremamente complesso e in perenne evoluzione, capace di assumere molteplici forme di manifestazione e mutare continuamente *modus operandi.*

L'incessante sviluppo dei *phishing attacks*, in ragione dell'impiego di tecniche sempre più sofisticate, innovative ed ingegnose, finalizzate a carpire i dati riservati degli utenti del *web*, rappresenta, attualmente, una vera e propria emergenza per la moderna società tecnologica, compromettendo i settori della sicurezza informatica e dei servizi finanziari.

Una significativa evoluzione del *phishing* è rappresentata dal c.d. "*pharming",* quale fenomeno consistente in una tecnica di *cracking* volta ad acquisire fraudolentemente, al pari della tradizionale forma di *phishing*, le

[413] Sul punto v. FLOR, Phishing, identity theft *e* identity abuse, cit., 933 ss.; v. anche DI VIZIO, Phishing: *le operazioni del prestaconto possono integrare il delitto di riciclaggio*, in *Quot. giur.* Web & Tech Phishing, che riporta Cass. Pen., Sez. II, 1° marzo 2017, n. 10060, in *www.pluris-cedam.utetgiuridica.it.*

informazioni personali degli utenti per diverse finalità, adottando un *modus operandi* distinto rispetto alla dinamica *standard*[414].

Tale tecnica di attacco comporta la manipolazione degli indirizzi *DNS*[415] che i soggetti cibernauti utilizzano per navigare sul *web*; tuttavia, al fine di cogliere i tratti salienti di tale tecnica, sembra opportuno fare una breve premessa sul funzionamento del servizio di rete.

Tutte le volte che l'utente inserisce nel proprio *browser* l'indirizzo di un sito *web* nella versione alfanumerica, il *server DNS* lo traduce in un indirizzo IP numerico allo scopo di raggiungere il *server* corrispondente a quel dominio[416].

Proprio il meccanismo funzionale alla risoluzione dei nomi alfanumerici in indirizzi IP può rappresentare un punto di vulnerabilità sfruttabile dal *pharmer*.

Il *pharming attack* è volto a modificare la corrispondenza numerica del dominio digitato, affinché i *server DNS* decifrino una corrispondenza numerica differente da quella reale e dirigano i cibernauti inconsapevoli ad un sito clone, solo apparentemente simile a quello reale, dirottando automaticamente tutti gli accessi ad una pagina appositamente creata, senza la necessità di cliccare su alcuna *mail*: così l'utente, credendo di inserire le credenziali di accesso sulla pagina *web* corretta, fornisce le stesse direttamente all'*hacker*.

Ad ogni modo, l'agente può decidere di attaccare un qualunque *DNS* del sistema di collegamento, sia esso il *DNS* del *provider* – come nel caso suesposto – o più semplicemente il *DNS* di un *computer* locale – nel qual caso la modifica avverrebbe direttamente all'interno del computer della vittima, con specifico

---

[414] V. CAJANI, COSTABILE, MAZZARACO, Phishing *e furto d'identità digitale,* cit., 37.

[415] *DNS* è l'acronimo di *Domain Name System.*

[416] Sul punto v. LOMBARDO, Pharming*: cos'è, come funziona e i consigli per difendersi dalla truffa dei "siti-trappola"*, in *www.cybersecurity360.it*, 28 gennaio 2020: più precisamente, il servizio di rete *DNS* opera mediante uno schema d'interrogazione gerarchico, per cui quando viene inserito l'*URL* di una pagina *web*, viene interpellato il *DNS* locale dell'elaboratore, o in alternativa, se le informazioni non risiedono localmente, il *DNS del provider*. Sono previste quattro distinte categorie di *server DNS*: *Resolver, Root Name server, TLD Name Sever e Name Server* autorevole. Qualora la risoluzione dell'indirizzo non sia presente sulla memoria del *Resolve*r, si attivano gli altri *server DNS*, ciascuno per la propria competenza, al fine di inviare al *client* l'indirizzo di dominio richiesto. Il procedimento di risoluzione degli indirizzi opera nella seguente modalità: Il Resolver DNS o interviene con i dati presenti sulla sua memoria o contatta un *nameserver root DNS* che lo indirizza ad un *nameserver TLD*, il quale a sua volta, a seguito di richiesta, reindirizza il Resolver verso un DNS autorevole in considerazione del nome di dominio; la richiesta finale è rivolta al *Name server* autorevole che comunica l'indirizzo IP richiesto al resolver, il quale provvederà a trasmettere la risposta definitiva al *client web.*

riguardo ai *file hosts*[417] o ai *file* di registro, grazie alla previa installazione di un *malware*[418] – , al fine di intercettare l'indirizzo IP equivalente al *domanin name* digitato dal soggetto ed elaborare un sito fittizio a cui ricondurre l'utente, funzionale ad ottenere i dati riservati dello stesso, compromettendo direttamente il sistema[419]

Si tratta di un attacco complesso, il cui *iter criminis* si sostanzia di numerose azioni poste in essere in momenti diversi. Il *pharming attack* opera direttamente ed illecitamente sul sistema DNS causando un'alterazione del funzionamento del sistema informatico o telematico; per tale ragione può astrattamente configurarsi il reato di frode informatica *ex* art. 640-*ter* c.p., che si concretizza con la realizzazione dell'evento di profitto, ovverosia con l'acquisizione dei dati riservati della vittima inconsapevole. Il seguente *login* all'*account* personale dell'utente può integrare gli estremi dell'accesso abusivo ad un sistema informatico o telematico ai sensi dell'art. 615-*ter*.

La maggiore insidiosità del *pharming* rispetto al tradizionale *phishing attack* deriva dal fatto che in tal caso non vi è la necessità di alcuna *e-mail* "esca" che induca il soggetto a collegarsi ad un *link* fittizio e ad inserire le proprie credenziali, poiché si agisce direttamente sul sistema, infatti anche i più attenti alla sicurezza potrebbero essere vittima di tale attacco; inoltre, l'elaboratore normalmente non viene infettato e l'evidenza dell' attacco può essere eliminata ristabilendo le tabelle *DNS* dei *server*, ragion per cui risulta sempre più compromesso il successo delle indagini[420].

L' aumento della presenza dei *malware* ha fortemente inciso sulla crescita del fenomeno del *pharming*, rendendolo altresì molto più pericoloso rispetto al *phishing* tradizionale. Negli ultimi anni questa tipologia di attacco è stata sempre

---

[417] LOMBARDO, Pharming*: cos'è, come funziona*, cit.: «Il *file host* [...] altro non è che un elenco di indirizzi alfanumerici risolti in indirizzi IP[...]. Il file viene utilizzato dai pc per gli accessi successivi senza dover richiedere l'indirizzo IP al *server DNS*. Una modifica non autorizzata degli indirizzi archiviati può di fatto reindirizzare il traffico verso il sito web contraffatto piuttosto che verso quello ufficiale».

[418] In argomento v. DEL NINNO, *Il furto di identità*, in CENDON (diretto da), *Trattato breve dei nuovi danni. Figure emergenti di responsabilità*, Vol. 3, Padova, 2014, 545.

[419] Sul punto v. CAJANI, COSTABILE, MAZZARACO, Phishing *e furto d'identità digitale,* cit., 38 s.

[420] *Ivi*, 39.

più spesso realizzata con innovative tecniche di *rootkit*[421], le quali hanno decisamente agevolato la posizione dell'*hacker,* causando non poche difficoltà ai sistemi di protezione *anti-malware*.

Al contempo, l'evoluzione del *phishing*, dovuta all'utilizzo di tecniche sempre più sofisticate, ha determinato l'insorgenza e lo sviluppo di ulteriori ed innovative varianti del fenomeno, tutte funzionali a capire i dati sensibili degli utenti in rete.

Tra le più rilevanti nuove forme di attacco si ravvisa il *vishing*[422], anche detto "*phishing* vocale", attraverso cui l'agente approfitta della sensibilità del soggetto destinatario di false comunicazioni urgenti, generalmente riferite a problematiche legate al conto corrente, per indurlo a digitare un determinato numero telefonico, collegato ad un *call center*, apparentemente volto a risolvere le suddette complicazioni, con il fine ultimo di acquisire i suoi dati sensibili.

Nella gran parte dei casi, il *visher* attiva un account VoIP e si serve di un sistema di chiamata automatico e di un nastro registrato, indirizzato ad un elevato numero di vittime, per effettuare l'avviso e indicare i passaggi da seguire per porre fine al problema segnalato[423].

Il *call center* che risponde alla vittima ignara, a seguito di chiamata, si mostra capace di risolvere ogni questione, previa comunicazione dei dati riservati, specialmente il numero di conto corrente e il numero di carte di credito.

La tecnologia *VoIP* utilizzata per sferrare l'attacco in questione «consente agli utenti di avere un numero telefonico geografico presso il quale ricevere ed effettuare chiamate, con l'unica eccezione che la voce viene veicolata mediante *Internet Protocol*, ossia il protocollo di comunicazione adoperato dalla rete

---

[421] Cfr. LEANDRO, Rootkit*: cosa sono, come individuarli e come rimuoverli*, in *www.cybersecurity360.it* ,10 luglio, 2019: «I *rootkit* sono una seria minaccia ai sistemi informatici, incasellabili nella categoria dei *malware*. [...] sono dei *kit*, ovvero strumenti o insiemi di strumenti, come sequenze di macro o veri e propri *software*, atti ad ottenere sul computer bersaglio i permessi di *root*, senza ovviamente che il proprietario del sistema oggetto dell'attacco ne sia a conoscenza [...]. Di fatto, installare un *rootkit* su una macchina, significa avere pieno possesso della stessa, potendo far compiere qualunque operazione si voglia».

[422] Il termine "*vishing"* deriva dall'unione dell'acronimo "*VoIP" (Voice over Internet Protocol*) e della parola "*phishing*": v. TRUNFIO, CRISAFI, *Il* phishing, cit., 968.

[423] *Ibidem*: può capitare che il *visher,* anziché attivare un *account VoIP* ed avviare un sistema di chiamata automatico, decida di agire inviando una *e-mail* ingannatoria con cui induce l'utente a cliccare su un l*ink,* e solo successivamente a comporre il numero telefonico connesso al falso *call center,* che gli chiederà di comunicare i dati personali che lo riguardano.

Internet. Questa tecnologia, oltre ad un considerevole risparmio sui costi, consente di ricevere ed effettuare chiamate da numeri con prefissi geografici riferiti a determinati distretti pur non trovandosi fisicamente in quei determinati distretti»[424].

Negli ultimi anni si è registrato un notevole aumento del fenomeno dei falsi *call center* su VoIP, poiché le vittime ripongono una maggiore fiducia nei confronti di chi effettua una comunicazione vocale rispetto a chi, invece, invia *e-mail*, percepite con maggiore diffidenza, sebbene in entrambi i casi il soggetto agente sia un truffatore[425].

Un'ulteriore variante del *phishing* che va diffondendosi è lo *smishing*[426], un tipo di attacco perpetrato tramite *sms*, volto ad ottenere i dati riservati e finanziari dei soggetti prescelti. La modalità di realizzazione di tale attacco è analoga a quella del *phishing* tradizionale, anche se al posto dell'*e-mail* viene inviato un messaggio telefonico – c.d. "*sms"* – con cui lo *smisher,* fingendosi una fonte affidabile, invita la potenziale vittima a chiamare un numero di telefono o a cliccare sul *link* indicato, e a connettersi al sito *web* per approfittare di un'offerta o di un servizio, ovvero per risolvere una determinata problematica insorta, esortandolo ad inserire i dati riservati, che verranno successivamente utilizzati dal criminale. Il soggetto che chiama il numero telefonico indicato nell'*sms* viene sollecitato da un risponditore automatico a fornire informazioni private, le stesse che è invitato ad inserire sul sito *web* a cui rinvia il *link* riportato nel messaggio, che riproduce la grafica e il contenuto di pagine *web* reali.[427]

Si tratta di un fenomeno che sfrutta le tecniche di ingegneria sociale, come si evince dal testo dei messaggi inviati, e che ha registrato un forte aumento di casi, in ragione del sempre maggiore utilizzo che viene fatto degli *smartphone*, divenuti ormai dei veri e propri contenitori di dati personali.

---

[424] Cfr. PERRI, *Lo* smishing *e il* vishing*, ovvero quando l'unico limite all'utilizzo criminale delle nuove tecnologie è la fantasia*, in *Dir. Internet*, 2008, 3, 266.

[425] TRUNFIO, CRISAFI, *Il* phishing, cit., 968.

[426] Il termine *smishing* deriva dall' unione dell'acronimo "*sms*" (*short message service*) e della parola "p*hishing":* v. TARSITANO, Smishing*: cos'è e come funziona il* phishing *che usa gli sms come esca*, in *www.cybersecurity360.it,* 4 dicembre 2018.

[427]Per approfondire sul punto v. TARSITANO, Smishing*: cos'è e come funziona* il phishing *che usa gli sms come esca*, cit.

In riferimento allo *smishing* assume particolare rilevanza il caso di truffa "CartaSì", affrontato dal Tribunale di Milano nel 2007[428]. A tal proposito, seppur brevemente, sembra opportuno inquadrare l'episodio in fatto e in diritto.

A partire dal gennaio 2006, numerosi titolari di carte di credito CartaSi avevano ricevuto degli sms, apparentemente provenienti dall'ente emittente "CartaSi", il cui testo invitava i soggetti a chiamare un numero telefonico di servizi interbancari per verificare una determinata operazione realizzata con la carta stessa, allo scopo di impedirne un uso fraudolento. Dalle indagini effettuate dalla Polizia postale di Milano si era risaliti all'identità di un soggetto già precedentemente indagato e condannato per fatti simili e connessi all'utilizzo indebito di carte di credito *on-line*; era stato altresì accertato che sul computer dell'indagato erano presenti *software* in grado di effettuare e ricevere telefonate VoIP per mezzo di un risponditore automatico capace di acquisire tutti i dati delle carte di credito, e che gli sms erano stati inviati da lui alle vittime, le quali poi avevano fornito i suddetti dati; inoltre, era stato appurato che, a seguito del fraudolento ottenimento delle informazioni sulle carte, le stesse erano state utilizzate per fare acquisti *on-line*[429].

Il GUP del tribunale di Milano ha condannato lo *smisher* a due anni e otto mesi di reclusione e a mille euro di multa, ritenendo sussistenti i seguenti reati: il reato di sostituzione di persona di cui all'art. 494 c.p., in ragione del fatto che l'imputato, mediante sms, aveva indotto in errore numerosi soggetti, sostituendo illegittimamente il proprio nome con quello di "Cartasi", con l' obiettivo di ottenere un vantaggio per sé o per altri[430]; il reato di truffa *ex* art. 640 c.p., poiché le vittime,

---

[428] Sentenza emessa dal Trib. di Milano, Ufficio GUP, 15 ottobre 2007 (depositata il 7 novembre 2007), a seguito di giudizio abbreviato: v. CAJANI, COSTABILE, MAZZARACO, Phishing *e furto d'identità digitale,* cit., 178 ss.

[429] V. CAJANI, COSTABILE, MAZZARACO, Phishing *e furto d'identità digitale,* cit., 178 ss.

[430] Cfr. PERRI, *Lo* smishing *e il* vishing, cit., 267: non sono mancate critiche circa l'effettiva applicabilità dell'art. 494 c.p. al fatto in esame, poiché secondo alcuni in tal caso «*in primis*, [...]non è possibile individuare un riferimento indicativo o distintivo di un soggetto "persona fisica" così come, invece, dovrebbe avvenire nel delitto in esame. *In secundis*, l'utilizzo sui siti *web* di dati personali o credenziali d'autenticazione di un determinato soggetto per l'accesso a determinati servizi, [...] non configurerebbe né la materiale sostituzione di una persona né l'attribuzione di un falso nome, di un falso stato o di una qualità cui la legge attribuisce effetti giuridici. *In tertiis,* [...] pur ammettendo un'interpretazione estensiva e forzata dei requisiti della norma, [...] rimane insuperabile l'ostacolo costituito dall'evento consumativo del reato, rappresentato dall''induzione in errore di taluno che non è in alcun modo compatibile o applicabile all'esecuzione automatizzata

tramite l'sms e il messaggio vocale, all'apparenza provenienti dal suddetto ente, erano state indotte a fornire i dati relativi alle carte di credito, al fine di procurarsi un vantaggio con altrui danno[431]; il reato di indebito utilizzo di carte di credito[432], in virtù del fatto che in non pochi casi si era ravvisato ad opera dello *smisher* un uso senza diritto delle succitate carte per fare acquisti in rete, sebbene sia stato evidenziato che per l'esistenza del reato è sufficiente l'illecita acquisizione o il mero possesso degli estremi di carte di credito di origine illecita con lo scopo di trarne profitto[433].

Dunque, la sentenza in esame afferma che «commette reato di sostituzione di persona, truffa e utilizzo indebito di carte di credito chi illecitamente sottrae numeri di carte di credito inviando a diversi soggetti *sms* ingannevoli nei quali, prospettando acquisti mai effettuati dai legittimi titolari, invita questi ultimi a contattare un numero telefonico dove una voce registrata, spacciandosi per il *call center* dell'istituto emittente, richiede i dati delle suddette carte. I dati così raccolti, in alcuni casi, sono utilizzati per effettuare degli acquisti»[434].

Tra le tecniche di attacco *phishing* più innovative vi sono anche il *fast flux e il tabnabbing.* Il primo è un metodo che permette di cambiare costantemente, a brevi intervalli di tempo, gli indirizzi *IP* e *domain server* degli elaboratori contaminati da *virus* e usati per accogliere siti di *phishing*. La principale utilità che l'*hacker* trae dall'utilizzo di questa tecnica consiste nella possibilità di ostacolare

di richieste inoltrate ai sistemi informatici. Date tali premesse, potrebbe apparire poco felice la scelta del giudice che, nella sentenza in esame, ritiene provato il reato di cui all'art. 494 c.p.».

[431] Cfr. PERRI, *Lo* smishing *e il* vishing, cit., 268: secondo alcuni «nella sentenza in esame, viene ravvisato il delitto di truffa, sebbene nulla vieterebbe, [...], l'individuazione di una frode informatica, soprattutto tenuto conto dell'ampiezza della formula usata dal legislatore per cui ricade in questa fattispecie pure chi interviene senza diritto su dati, informazioni o programmi anche solo "pertinenti" ad un sistema informatico o telematico».

[432] Tale reato è stato inserito nel codice penale dall'art. 4 del D.lgs. 21/2018, prima di allora il fatto era sanzionato ai sensi dell'art. 12 della legge n. 197 del 1991, successivamente sostituito dall'art 55, comma 9, del D.lgs. n.231/2007: sul punto v. *supra* § 2.1.

[433] Cfr. PERRI, *Lo* smishing *e il* vishing, cit., 268: «Sia la sostituzione di persona che la truffa risultano, secondo il giudice, teleologicamente connesse all'utilizzo indebito di carte di credito per conseguire un ingiusto profitto. Emerge quindi come aspetto rilevante della sentenza l'elemento dell'ingiusto profitto con altrui danno, che nel caso di specie si integrava mediante l'utilizzo, al fine di acquistare beni su internet, dei numeri di carte di credito e dei codici di verifica di queste ultime illecitamente sottratti».

[434] Cfr. PERRI, *Lo* smishing *e il* vishing, cit., 261.

l'identificazione dei siti clone da parte delle autorità, evitando così la loro successiva chiusura[435].

L'*hacker* invia all'utente una *e-mail* avente ad oggetto un *link*, appartenente alla *botnet-fastflux*; la vittima, confidando nell'autenticità della pagina a cui è rinviata, immette le proprie credenziali e, subito dopo, viene reindirizzata automaticamente al sito reale, affinché non si accorga di nulla.

Il *tabnabbing*, invece, è una forma di *phishing* finalizzata a carpire fraudolentemente i dati personali degli utenti mediante l'apertura contestuale di pagine-trappola e reali; la vittima inconsapevole, dopo aver fornito le informazioni d' interesse all'agente, come richiesto dal sito fittizio, viene condotta all'indirizzo originale.

Ebbene, dall'esame del fenomeno del *phishing* sin qui svolto si evince chiaramente che nel corso degli anni tale tecnica di attacco si è evoluta ed affinata, dando origine a condotte sempre più complesse e difficili da contrastare con le attuali misure di carattere tecnico e normativo, mostratesi decisamente insufficienti. Si auspica, pertanto, un intervento *ad hoc* del legislatore, affinché il fenomeno del *phishing* possa essere, in futuro, espressamente previsto e sanzionato, sebbene non debba essere sottovaluta l'importanza della diffusione di una cultura informatica attenta ed aggiornata, quale principale strumento di contrasto alla criminalità cibernetica.

[435] Per approfondire sul punto v. CAJANI, COSTABILE, MAZZARACO, Phishing *e furto d'identità digitale,* cit., 41 ss.

CONCLUSIONI

Giunti al termine della presente trattazione, sembra opportuno proporre un riepilogo delle conclusioni a cui si è giunti nel corso dell'elaborato.

Innanzitutto è bene premettere che, al fine di cogliere la reale entità e gravità del fenomeno delle truffe *on-line*, nella parte inziale del lavoro si è posta in evidenza la rilevanza e la significatività dell'evoluzione tecnologica nel contesto sociale e giuridico, sottolineando come la formazione di una nuova dimensione abbia comportato non solo l'introduzione di numerosi profili di vantaggio e innovazione, bensì anche inevitabili aspetti critici, propri di una realtà diversa da quella materiale, connotata da elementi digitali intrinsecamente pericolosi, le cui caratteristiche principali si ravvisano nell'astrattezza, rapidità, atemporalità, dematerializzazione e aterritorialità.

Gli utenti, quindi, risultano costantemente esposti al rischio di minacce di attacchi cibernetici sempre più complessi e sofisticati, nonché all'eventualità di essere vittime di *cybercrimes*, e più precisamente di uno dei reati riconducibili alla categoria generale delle truffe *on-line*.

Dopo aver approfondito la questione concernente le diverse concezioni di patrimonio elaborate dalla dottrina penalistica si è affermata la condivisibilità della definizione giuridico-funzionale, la quale ricomprende nella suddetta nozione, al di là del valore strettamente economico, anche il valore di affezione.

Le condotte realizzate nel *cyberspace* si traducono in una serie di operazioni automatizzate, rispetto alle quali risulta piuttosto problematico adattare i criteri giuridici tradizionali, ragion per cui, nel corso dell'esame delle truffe perpetrate a mezzo *web*, si è invocato l'intervento del legislatore, anche a causa delle difficoltà applicative riscontrate nel tentativo di estendere il reato di truffa tradizionale, di cui all'art. 640 c.p., ad un diverso contesto d'azione, qual è, appunto, il cyberspazio.

È emerso che, alla luce della dematerializzazione e degli automatismi, nella truffa commessa *on-line* la portata dell'essenziale elemento di cooperazione artificiosa sembrerebbe subire un ridimensionamento, poiché difetta il contatto diretto tra le parti.

La rete, fungendo da "filtro" digitale, da un lato consente una più semplice predisposizione dell'inganno tipico del reato, e dall'altro rende più complicato il riconoscimento della condotta truffaldina per il soggetto passivo, causando così una più grave offesa ai beni giuridici coinvolti.

Si è poi sottolineato che molti degli autori di truffe telematiche, in ragione delle inadeguatezze di cui si è detto, rischiano di rimanere impuniti, per cui sarebbe auspicabile un intervento legislativo *ad hoc* per contrastare distintamente e definitivamente la condotta truffaldina perpetrata a mezzo *web*.

È risultato, inoltre, che il contesto prediletto per la commissione delle truffe *on-line* è quello delle piattaforme *e-commerce* e degli *on-line criminal markets*, i quali agevolano la condotta del truffatore.

Nella seconda parte del secondo capitolo si è affrontata la disamina relativa alla fattispecie di frode informatica, introdotta dal legislatore con la legge n. 547 del 1993; al riguardo, sono state evidenziate in particolar modo le analogie e le differenze tra il suddetto delitto di frode e il delitto di truffa, nonché tra questi e gli altri reati cibernetici, precisando che i fatti connessi all'informatica in cui vi è induzione in errore di un soggetto devono essere ricondotti all'art. 640 c.p., mentre quelli in cui si verifica un'alterazione o un intervento abusivo sul sistema informatico o telematico sono espressamente disciplinati dall'art. 640-*ter*.

Si è altresì affermata l'autonomia strutturale dei due reati, ritenendosi inammissibile qualunque rapporto di specialità tra le due fattispecie criminose.

Per quel che concerne l'annosa questione relativa alla determinazione del *locus commissi delicti* nelle truffe *on-line* si è specificato che essa è indissolubilmente legata alla determinazione del momento consumativo, come affermato dalla sentenza delle Sezioni Unite della Cassazione risalente alla fine degli anni '60, secondo cui la consumazione dei reati in esame si verifica con realizzazione del duplice evento consumativo, ovverosia con la definitiva *deminutio patrimonii* per il soggetto passivo e con il conseguimento dell'ingiusto profitto per l'agente. Come emerge dal testo, le diverse soluzioni prospettate in merito alla problematica del *locus commissi delicti* si fondano su differenti orientamenti interpretativi, e dipendono dal metodo di pagamento utilizzato dalla vittima.

Infine, nell'ambito delle truffe *on-line,* si è ribadita, nel terzo capitolo, l'importanza assunta dalle tecniche di *social engineering*, determinanti, in particolare, per la realizzazione e l'evoluzione del fenomeno del *phishing*. A tal riguardo sono state individuate le diverse fasi di cui esso di compone e, non ravvisandosi una disciplina giuridica specifica che consideri unitariamente il fenomeno, è stata contestualmente prospettata l'applicabilità di precise norme penali vigenti per ciascuna delle condotte tipiche realizzate.

Da ultimo, si è considerato il caso "CartaSì", rilevante esempio di *smishing*, la cui sentenza ha affermato che nel caso di specie si configurano i reati di sostituzione di persona, truffa e utilizzo indebito di carte di credito, sebbene in dottrina non sia stata esclusa la possibilità di applicare l'art. 640-*ter* che prevede la fattispecie di frode informatica.

Per concludere, anche in riferimento al *phishing* si è auspicato un intervento legislativo *ad hoc*, che tenga conto dell'unicità e della dinamicità del fenomeno, nonché dell'incessante evoluzione tecnologica da cui esso dipende.

Alla luce dell'analisi svolta, quindi, emerge che quella delle truffe *on-line* è una categoria che ricomprende diversi reati, che, a parere di chi scrive, per essere efficientemente contrastati dovrebbero essere oggetto di un apposito intervento normativo, finalizzato a prevedere e disciplinare precisamente ciascuno di essi. Come si è avuto modo di sottolineare nel corso della trattazione, attualmente l'intervento del legislatore ha riguardato solo l'introduzione della fattispecie di frode informatica, volta a punire chi realizza una condotta fraudolenta nei confronti di un sistema informatico o telematico.

Sembra chiaro, pertanto, che in una prospettiva *de iure condendo*, la fattispecie che, in ragione dell'innovazione tecnologica e dell'avvento del *cyberspace*, necessiterebbe maggiormente di essere integrata o comunque riformulata è quella della truffa *ex* art. 640 c.p., poiché l'analisi svolta ha evidenziato che, sebbene gli elementi costitutivi siano i medesimi del reato tradizionalmente previsto, la truffa perpetrata a mezzo *web* presenta una più intensa potenzialità offensiva, e perciò un maggior disvalore penale a fronte di una condotta fraudolenta meno impegnativa, essendo l'agente facilitato alla commissione della

stessa dalle tipicità del *web*; sarebbe addirittura auspicabile l'introduzione di una norma *ad hoc* che disciplini esclusivamente la truffa commessa *on-line*.

Perciò, i profili caratteristici della fattispecie di cui all'art. 640 c.p., al fine di punire i *cyber*-truffatori e soddisfare le possibili nuove esigenze di maggior tutela, dovrebbero essere ridefiniti alla luce delle suddette tipicità digitali, nonché della continua evoluzione del contesto informatico in cui il reato in questione viene commesso.

Infine, con riguardo alla frode informatica, in accordo con parte della dottrina, si ravviserebbe la necessità di un rimodellamento della norma, in virtù dell'ampiezza della formula usata dal legislatore del '93; mentre, sempre ad avviso di chi scrive, il fenomeno del *phishing*, in ragione dell'autonoma dimensione offensiva, dovrebbe essere previsto da una disciplina unitaria, e non da una sorta di addizione normativa realizzata sulla base delle diverse e numerose condotte di cui il fenomeno stesso si compone.

Con il presente elaborato, quindi, si è voluto affrontare un tema attuale e innovativo, poiché le truffe *on-line* rappresentano un vero e proprio allarme sociale per il singolo e per la collettività, sebbene, come è emerso nel corso della trattazione, per contrastare tali crimini cibernetici offensivi del patrimonio non possa prescindersi dall'applicazione dei tradizionali principi del diritto penale, i quali però, come si è detto, dovrebbero essere correttamente adeguati al particolare contesto di realizzazione.

INDICE BIBLIOGRAFICO

ACCINNI, *Profili di responsabilità penale dell'*hosting provider *"attivo"*, in *Arch. pen.*, 2017, 2, 2.

AMATO, DESTITO, DEZZANI, SANTORIELLO, *I reati informatici. Nuova disciplina e tecniche processuali di accertamento*, Padova, 2010.

ANTOLISEI, *Manuale di diritto penale. Parte speciale*, Vol. I, 16 ª ed Milano, 2016.

BALLONI, BISI, SETTE, *Principi di criminologia applicata. Criminalità, controllo, sicurezza*, Padova, 2015.

BERGHELLA, BLAIOTTA, *Diritto penale dell'informatica e beni giuridici*, in *Cass. pen.*, 1995, 9, 1463.

CAJANI, COSTABILE, MAZZARACO, Phishing *e furto d'identità digitale: indagini informatiche e sicurezza bancaria*, Milano, 2008.

CAMPEIS, *La frode informatica*, in CENDON (diretto da), *Trattato dei nuovi danni, informazioni erronee, soggetti deboli, illeciti informatici, danni ambientali*, Vol. V, Padova, 2011, 917.

CAPONE, *Gli attacchi di ingegneria sociale*, in *www.cyberlaws.it*, 8 marzo 2018.

CAPONE, *Le principali tipologie di "*phishing attac*k"*, in *www.cyberlaws.it*, 27 giugno 2018

CARMONA, *I reati contro il patrimonio,* in FIORELLA (a cura di), *Questioni fondamentali della parte speciale del diritto penale. Estratto ad uso degli studenti Università degli studi "Sapienza"*, 3ª ed., Torino, 2019, 2.

CEDROLA, *I reati informatici: le truffe* on-line, in *www.iusinitinere.it,* 18 gennaio 2017.

CIACCI, *L'ordinamento giuridico e le fonti del diritto dell'informatica*, in VALENTINO (a cura di), *Manuale di diritto dell'Informatic*a, Napoli, 2011, 7.

CIPOLLA, E-commerce *e truffa,* in *Giur. merito,* 2013, 12, 2624.

CONIGLIARO, *La nuova tutela penale europea dei sistemi di informazione. Una prima lettura della direttiva 2013/40/UE del Parlamento europeo e del Consiglio,* in *Dir. pen. cont.*, 30 ottobre 2013, 1.

CUOMO, RAZZANTE, *La disciplina dei reati informatici*, Torino, 2007.

CUOMO, RAZZANTE, *La nuova disciplina dei reati informatici*, Torino, 2009.

DAL CHECCO, Il ransomware Wannacry *infetta PC non aggiornati: ospedali ed enti pubblici a rischio,* in *www.ransomware.it,* 12 maggio 2017.

DEL NINNO, *Il furto di identità,* in CENDON (diretto da), *Trattato breve dei nuovi danni. Figure emergenti di responsabilità*, Vol. 3, Padova, 2014, 537.

DI PRISCO, *Truffe* on-line *e Postepay: quando e dove si consuma il reato? in www.iusinitinere.it, 29* gennaio, 2018.

DI VIZIO, Phishing: *le operazioni del prestaconto possono integrare il delitto di riciclaggio,* in *Quot. giur. Web&Tech* Phishing, *27 marzo 2017.*

FANELLI, *Telefonate abusive e frode informatica*, in *Foro it.*, 1999, 10, 608.

FARINA, *Elementi di diritto dell'informatica*, Padova, 2019.

FIANDACA, MUSCO, *Diritto penale. Parte speciale*, Vol. II, 7ª ed., Bologna, 2015.

FLOR, Phishing, identity theft *e* identity abuse. *Le prospettive applicative del diritto penale vigente*, in *Riv. it. dir. proc. pen.*, 2007, 2-3, 899.

FLOR, *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di internet,* in *Dir. pen. cont.*, 20 settembre 2012, 1.

FLOR, *I limiti del principio di territorialità nel cyberspace. Rilievi critici alla luce del recente orientamento delle Sezioni Unite*, in *Dir. pen. proc.*, 2015,10 1291.

FLOR, Cyber-criminality*: le fonti internazionali ed europee*, in CADOPPI, CANESTRARI, MANNA, PAPA (diretto da), Cybercrime, Torino, 2019, 98.

FLOR Cybersecurity *ed il contrasto ai* cyber-attacks *a livello europeo: dalla CIA*-Triad protection *ai più recenti sviluppi*, in *Riv. dir. Internet*, 2019, 3, 453.

FLOR *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in CADOPPI, CANESTRARI, MANNA, PAPA (diretto da), Cybercrime, Torino, 2019, 141.

FOGLIANI, *I reati commessi su internet:* computer crimes *e* cybercrimes, in *www.fog.it*, 3 marzo 2009.

GIORDANO, *Presupposti e limiti all'utilizzo del captatore informatico: le indicazioni della Suprema Corte*, in *Sist. Pen*, 2020, 4, 109.

IASELLI, *Sicurezza nazionale cibernetica: il decreto-legge coordinato in Gazzetta, in www.altalex.it*, 25 novembre 2019.

INGRASSIA, *Il ruolo dell'ISP nel cyberspazio: cittadino, controllore o tutore dell'ordine?*, in *Dir. pen. cont*., 8 novembre 2012, 1.

LEANDRO, Rootkit*: cosa sono, come individuarli e come rimuoverli*, in *www.cybersecurity360.it*, 10 luglio 2019.

LOMBARDO, Spyware*: cosa sono, come si diffondono e come eliminarli, in www.cybersecurity360.it*, 16 Maggio 2019.

LOMBARDO, Pharming*: cos'è, come funziona e i consigli per difendersi dalla truffa dei "siti-trappola", in www.cybersecurity360.it*, 28 gennaio 2020.

LUBERTO, "Sex-Torsion" *via web e minaccia a mezzo ransomware: la nuova frontiera del delitto di estorsione*, in CADOPPI, CANESTRARI, MANNA, PAPA (diretto da), Cybercrime, Torino, 2019, 724.

LUCARELLI, *Le truffe*, in CENDON (a cura di), *La prova e il quantum nel risarcimento del danno non patrimoniale*, Torino, 2008, 1993.

LUPÁRIA, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa. I Profili processuali*, in *Dir. pen. proc*., 2008, 6, 717.

MALAGNINO, *Sostituzione di persona e* web*: le false recensioni* online, in *Giur. pen. web*, 2019, 4, 1.

MALETTA, *Il lato oscuro dell'*e-commerce *e i nuovi reati digitali: dalla truffa online alla frode informatica*, in *Salvis juribus*, 11 giugno 2020.

MARINUCCI, DOLCINI, *Costituzione e politica dei beni giuridici*, in *Riv. it. dir. proc. pen.*, 1994, 2, 333.

MARRA, *Truffa*, in FIORE (diretto da), *I reati contro il patrimonio*, Torino, 2010, 477.

MARTINO, *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in *Politica&Società*, 2018, 1, 61.

MARTONE, *Il delitto di truffa nella recente giurisprudenza: la dibattuta questione della c.d. truffa processuale*, in *De Iustitia*, 2017, 4, 150.

MARZULLO, *Truffa informatica*, in *Arch. Pen.*, 2017, 3, 2.

MASI, *Frodi informatiche e attività bancaria*, in *Riv. pen. econ.*, 1995, 4, 427.

MENSI, *La sicurezza cibernetica*, in MENSI, FALLETTA, *Il diritto del web*, Padova, 2018, 281.

MEZZALAMA, LIOY, METWALLEY, *Anatomia del* malware, in *Riv. Mondo Digitale*, 2013, 47, 1.

MEZZETTI, *Reati contro il patrimonio*, in GROSSO, PADOVANI, PAGLIARO (diretto da), *Trattato di diritto penale. Parte speciale*, XV, Milano, 2013, 461.

MINICUCCI, *Le frodi informatiche*, in CADOPPI, CANESTRARI, MANNA, PAPA (diretto da), Cybercrime, Torino, 2019, 827.

MORALES GARCÌA, *La politica criminale nel contesto tecnologico. Una prima approssimazione alla Convenzione del Consiglio d'Europa sul* Cyber-Crime, in PICOTTI (a cura di), *Il diritto penale dell'informatica nell' epoca di internet*, Padova, 2004, 123.

NERI, *Criminologia e reati informatici. Profili di diritto penale dell'economia*, Napoli, 2014.

PANATTONI, Compliance, cybersecurity *e sicurezza dei dati personali*, Assago, 2020.

PARODI, *La frode informatica: presente e futuro delle applicazioni criminali nell' uso dei* software, in *Criminalità informatica*, a cura di SARZANA DI SANT'IPPOLITO, in *Dir. pen. proc.*, 1997, 12, 1538.

PATI, E-commerce*, che cos'è e come funziona: regole 2020*, in *www.agendadigitale.eu*, 5 giugno 2020.

PECORELLA, *Diritto penale dell'informatica. Ristampa con aggiornamento*, Padova, 2006.

PECORELLA, *Truffe* on-line*: momento consumativo e competenza territoriale*, in *Dir. pen. cont*., 10 maggio 2012, 1.

PECORELLA, *I reati informatici contro il patrimonio*, in PULITANÒ (a cura di), *Diritto penale. Parte speciale. Volume II. Tutela penale del patrimonio*, Torino, 2013, 271.

PECORELLA, DOVA, *Profili penali delle truffe* on-line, in *Arch. pen.*, 2013, 3, 799.

PERRI, *Lo* smishing *e il* vishing*, ovvero quando l'unico limite all'utilizzo criminale delle nuove tecnologie è la fantasia*, in *Dir. Internet*, 2008, 3, 261.

PICA, *Diritto penale delle tecnologie informatiche*, Torino, 1999.

PICOTTI, *Presentazione*, in PICOTTI (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet,* Padova, 2004, VII.

PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in PICOTTI (a cura di), *Il diritto penale dell'informatica nell'epoca di internet*, Padova, 2004, 21.

PICOTTI, *La ratifica della Convenzione* Cybercrime *del Consiglio d'Europa, Profili di diritto penale sostanziale*, in *Dir. pen. proc.*, 2008, 6, 700.

PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, in CADOPPI, CANESTRARI, MANNA, PAPA (diretto da), Cybercrime, Torino, 2019, 35.

PIVATO, Lo spam*: cos'è e come difendersi, anche alla luce del GDPR,2019,* in *www.cybersecurity 360.it*, 13 novembre 2019.

PICOTTI, VADALÀ, *Sicurezza cibernetica: una nuova fattispecie delittuosa a più condotte con estensione della responsabilità degli enti*, in *Sist. pen.*, 5 dicembre 2019.

PINO, Phishing - *Cassazione Penale: risponde di frode informatica l'intestatario della carta prepagata utilizzata per attività di* phishing, in *www.filodiritto.it*, 29 novembre 2018.

RIJTANO, Keylogger*: cos'è, come eliminarlo, i migliori per Windows, Mac e cellulare*, in *www.cybersecurity360.it, 24 maggio 2018.*

RIJTANO, SBARAGLIA, WannaCry*, cos'è, come funziona e come difendersi dal* ransomware *che ha fatto piangere il mondo, in www.cybersecurity360.it*, 28 giungo, 2018.

RIJTANO, Cryptolocker*, cos'è, come si prende e come difendersi*, in *www.cybersecurity360.it,* 2 luglio 2018.

RONCO, ROMANO, *Codice penale commentato,* 4ª ed., Torino, 2012.

SANTORO, *Il progetto internazionale "*No more ransom" *alla luce dell'attacco* WannaCry, in *Quot. giur.* Web&Tech *Sicurezza informatica,* 1° giugno 2017.

SARZANA DI SANT'IPPOLITO, *Problemi vecchi e nuovi nella lotta alla criminalità informatica*, in PICOTTI (a cura di), *Il diritto penale dell'informatica nell'epoca di internet*, Padova, 2004, 3.

SARZANA DI S. IPPOLITO, *Informatica, Internet e diritto penale,* (terza edizione, riveduta, corretta ed ampliata), Milano, 2010.

SCOPINARO, *Internet e reati contro il patrimonio*, Torino, 2007.

SENOR, *Come funzionano i* trojan *di stato? Analisi delle nuove norme e indicazioni operative, in www. altalex.com*, 22 gennaio 2018.

SETOLA, ASSENZA, *Recepimento della Direttiva NIS sulla* cybersecurity *delle reti*, in *www. sicurezzaegiustizzia.com*, 20 gennaio 2019, 32.

SEVERINO, *Standard globali in difesa della trasformazione digitale*, in *www.ilsole24ore.com*, 29 marzo 2019.

SILVETTI, *I crimini informatici più frequenti degli ultimi anni: tabella riepilogativa e profili giuridici*, in *Quot. giur.*, 4 ottobre, 2019.

SIRILLI, *voce Innovazione tecnologica, in Enc. della scienza e della tecnica*, 2008, reperibile su *www.treccani.it*.

SIRILLI, voce *Società dell'informazione, in Enc. della scienza e della tecnica*, 2008, *www.treccani.it*.

STALLA, *L'accesso abusivo ad un sistema informatico o telematico*, in *www.penale.it*.

TARSITANO, Smishing: *cos'è e come funziona il* phishing *che usa gli sms come esca*, in *www.cybersecurity360.it*, 4 Dicembre 2018.

TARSITANO, Ginp, il trojan Android *che finge di segnalare i contagiati da Coronavirus*, in *www.cybersecurity360.it*, 25 marzo 2020.

TRUNFIO, CRISAFI, *Il* phishing, in CENDON (diretto da), *Trattato dei nuovi danni, informazioni erronee, soggetti deboli, illeciti informatici, danni ambientali*, Vol. V, Padova, 2011, 957.

VULPIANI, *La nuova criminalità informatica. Evoluzione del fenomeno e strategie di contrasto*, in *Riv. di criminologia, vittimologia e sicurezza*, Vol. I, n.1, 2007, 1.

ZANNOTTI, *La truffa*, Milano, 1993.

INDICE DELLA GIURISPRUDENZA

Cass. pen., 3 luglio 2009, n. 34059, rv. 244948.

Cass. pen., 11 novembre 2009, n. 44720, rv. 245696.

Cass. pen., 1° dicembre 2010, n. 24718, rv. 248662.

Cass. pen., 15 aprile 2011, n. 17748, rv. 250113.

Cass. pen., Sez. Un., 29 settembre 2011, n. 155, rv. 251499.

Cass, pen., Sez. II, 6 marzo 2013, n. 13475.

Cass. pen., 19 marzo 2013, n. 28703, rv. 256348.

Cass. Pen., Sez. II, 13 ottobre 2015 n. 50140.

Cass. pen., Sez. II, 29 settembre 2016, n. 43705.

Cass. pen., Sez. II, 20 ottobre 2016, n. 48027.

Cass. pen., Sez. II, 1° marzo 2017, n. 10060.

Cass. pen., Sez. VI, 10 aprile 2017, n. 17937.

Cass. pen., 6 ottobre 2017, n. 3329.

Cass. pen., Sez. II, 24 ottobre 2018, n. 48553.

Cass. pen., Sez. VI, 27 marzo 2019, n. 13411, rv. 275463-04.

Trib. Nola, 21 maggio 2020, n. 780.

Cass. pen., Sez. II, 29 maggio 2019, n. 26604.

Cass. pen., Sez. II, 20 dicembre 2019, n.51551, rv. 278231-01.

Corte App., Lecce, 7 settembre 2020, n. 602.

Corte App., Lecce, 9 settembre 2020, n. 506.

Cass. pen., Sez. V, 9 settembre 2020, n. 30726.

Cass. pen., Sez. II, 11 settembre 2020, n. 26589, rv. 279647-01.

Trib. Frosinone, 12 Settembre 2020, n. 795.

SITOGRAFIA

www.agendadigitale.eu

www.altalex.com

www.archiviopenale.it

www.coe.int

www.consob.it.

www.clusit.it

www.cyberlaws.it

www.cybersecurity360.it

www.dejure.it

www.diritto.it

www.dirittopenale.it

www.dirittopenalecontemporaneo.it

www.eurlex.it

www.eur-lex.europa.eu

www.exeo.it

www.fasi.biz

www.filodiritto.it

www.fog.it

www.gazzettaufficiale.it

www.giurisprudenzapenale.com

www.ilsole24ore.com

www.iusinitinere.it

www.ius-web.it

www.penale.it

www-pluris-cedam.utetigiuridica.it

www.ransomware.it

www.salvisjuribus.it

www.sicurezzaegisutizia.com

www.sicurezzait.gov.it

www.sicurezzanazionale.gov.it

www.treccani.it

www.webgiurdico.it

www.zerounoweb.it