RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2024 • DOI 10.32091/RIID0153 • articolo sottoposto a peer review • pubblicato in anteprima il 27 mag. 2024

Stefano Pietropaoli

Un'occasione (forse) mancata. Considerazioni sulla revisione dei reati informatici proposta con il DDL Cybersicurezza

L'Autore è professore associato di Filosofia del diritto presso l'Università degli Studi di Firenze

Questo contributo fa parte della sezione monografica *Il DDL Cybersicurezza (AC1717). Problemi e prospettive in vista del recepimento della NIS2* – Instant Book, a cura di Gaia Fiorinelli e Matteo Giannelli

Il disegno di legge 1717 propone un'articolata serie di interventi che mirano – anche grazie al rafforzamento delle funzioni dell'Agenzia per la cybersicurezza nazionale (ACN) – a consolidare la sicurezza informatica del Paese.

Mentre le disposizioni di cui al Capo I sono rivolte al conseguimento di una maggiore capacità di protezione e risposta alle emergenze cibernetiche, il Capo II è invece formulato con l'intenzione di garantire una maggiore tutela della persona e del patrimonio di fronte alle ormai diffusissime pratiche criminali svolte sul web (o comunque attraverso strumenti informatici).

Considerato il limitato spazio a disposizione, mi limiterò ad alcune brevi considerazioni generali in riferimento al Capo II, per rilevare poi quelle che mi sembrano le principali criticità del disegno di legge in oggetto.

Prima di tutto, il ddl prevede un generale innalzamento delle comminatorie edittali della quasi totalità dei reati (cosiddetti "necessariamente informatici") introdotti dalla legge 547 del 1993. Si tratta di un inasprimento delle sanzioni, anche molto rilevante, motivato – riprendendo le parole dell'analisi tecnico-normativa che accompagna il ddl – «dall'esigenza di realizzare una più intensa tutela dei beni finali […] fortemente esposti ad allarmanti forme di criminalità informatica».

Questa scelta di fondo appare, in via generale, condivisibile, se si considera il sempre maggiore disvalore delle condotte criminali nello spazio cibernetico. Tuttavia, preme sottolineare che il maggiore problema rappresentato dalle forme di criminalità informatica non consiste tanto nella loro offensività, quanto piuttosto nella effettiva perseguibilità degli illeciti perpetrati. Reati informatici e cybercrimes presentano, come è noto, enormi difficoltà nell'individuazione dei responsabili, che sempre più spesso si avvalgono di raffinate tecniche di offuscamento – VPN, reti Tor, tecnologie di crittografia – capaci di garantire un sostanziale anonimato. Frequentissimi, inoltre, sono gli illeciti commessi a partire da paesi stranieri (con

molti dei quali mancano efficaci accordi di cooperazione giudiziaria).

L'inasprimento delle sanzioni per queste tipologie di illeciti è dunque destinato a rimanere una soluzione insoddisfacente se non accompagnata da misure di diversa natura. Ancor più che nella realtà analogica, nello spazio cibernetico è fondamentale il ruolo della prevenzione. Ma non si ha efficace prevenzione senza conoscenza e consapevolezza. In altre parole, è indispensabile un'attenta opera di pianificazione e promozione di progetti formativi e iniziative di vera e propria "pedagogia digitale" – calibrati sulle diverse fasce di età, istruzione e mansioni – ma rivolti a tutta la popolazione, dalla prima età scolare alla terza età, dall'impiegato al dirigente, dal professionista al pensionato. In particolare, appare urgente prevedere un piano di sviluppo di competenze, strumenti e tecniche che possano rendere più efficace l'azione delle nostre forze dell'ordine, messe in sempre più grave difficoltà da reati davanti ai quali rimangono sostanzialmente impotenti.

Passando a considerazioni di diverso tenore, vorrei esprimere anche qualche perplessità di natura sistematica sull'impianto del ddl 1717.

Il punto più complesso riguarda a mio avviso la proposta di "abrogazione" dell'art. 615-*quinquies* e la sua sostanziale ricollocazione nell'alveo dei delitti di danneggiamento di dati e sistemi informatici ex artt. 635-*bis* e ss.

L'attuale formulazione dell'articolo 615-*quinquies*, effettivamente, ben si può intendere come disposizione normativa che sanziona le condotte dirette a danneggiare o interrompere un sistema informatico o telematico. Pertanto, in questa prospettiva, il suo inserimento quale nuovo art. 635-*quater*.1 è pienamente giustificato (tab. 1).

Testo vigente	Testo ddl 1717
Articolo 615-*quinquies* Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico	Articolo 635-*quater*.1 Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico.
«Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329».	«Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico ovvero le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici è punito con la reclusione fino a due anni e con la multa fino a euro 10.329».

Tab. 1

La ricollocazione della disposizione vigente ha senz'altro una giustificazione "tematica". Tuttavia, occorre ricordare che la non ottimale collocazione che possiamo riscontrare nel codice vigente è dovuta alle (non felici) riformulazioni – prima con la legge 18 marzo 2008, n. 48 e poi con la legge 23 dicembre 2021, n. 238 – del testo originale.

Occorre infatti ricordare che il legislatore del 1993 aveva effettuato una precisa scelta sistematica: in contiguità con l'articolo 614 (violazione di domicilio), veniva introdotto il reato di "violazione di domicilio informatico" (615-*ter*), accompagnato da altri due illeciti consistenti in condotte prodromiche a tale accesso abusivo: l'art. 615-*quater* e, appunto l'art. 615-*quinquies*.

Credo che sarebbe opportuno sì ricollocare la disciplina dell'attuale art. 615-*quinquies*, ma anche mantenere un reato tematicamente congruente con la scelta del 1993. In altre parole, pur tenendo ferma la ricollocazione del testo del vigente art. 615-*quinquies* come art. 635-*quater*.1, credo sarebbe opportuno modificare (e non abrogare) l'articolo 615-*quinquies* al fine di sanzionare anche le condotte di chi

"si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici", non animato dal dolo specifico di danneggiare illecitamente un sistema informatico o telematico etc., bensì dal dolo specifico di introdursi abusivamente in un sistema informatico o telematico.

Al fine di reintegrare il quadro di tutele originariamente previsto, sarebbe inevitabile il ripristino della disposizione di cui all'art. 615-*quater* alla versione originale.

Cercando di sbrogliare la matassa: ferma restando la ragionevolezza dell'introduzione di un reato (al nuovo art. 635-*quater*.1) che sanzioni, per esempio, l'installazione di programmi allo scopo di danneggiare illecitamente un sistema informatico o telematico, credo che sarebbe altrettanto ragionevole prevedere all'art. 615-*quater* il reato di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici, e al 615-*quinquies* il reato di detenzione, diffusione e installazione di apparecchiature, dispositivi o programmi informatici idonei all'accesso abusivo ad un sistema informatico o telematico.

Senza questo riassestamento complessivo, infatti, rimarrebbe "scoperta" l'ipotesi di chi installi un software malevolo capace di alterare – ma non danneggiare – il funzionamento di un determinato dispositivo con l'unico scopo di consentirne l'accesso abusivo.

Nella tab. 2 riporto, nella colonna di destra, le possibili modifiche agli artt. 615-*quater* e 615-*quinquies*.

Infine, vorrei segnalare l'aspetto che mi sembra più critico nel ddl in esame. Si tratta, in questo caso, della critica non di una nuova previsione, ma dell'assenza di una previsione.

Tra tutti gli illeciti informatici, infatti, quello che rappresenta il maggiore pericolo per la cittadinanza – e che viene commesso con maggiore frequenza – è il fenomeno delle truffe online. Secondo i dati ISTAT, truffa "analogica" e frode informatica ha raggiunto insieme lo straordinario numero di 300.000 denunce inoltrate in un anno all'autorità giudiziaria da parte Arma dei Carabinieri, Polizia di Stato e Guardia di Finanza, a fronte delle 35.000 denunce complessive per gli altri reati informatici.

È tuttavia opportuno sottolineare che il fenomeno comunemente indicato come "truffe online" è estremamente variegato e di non semplice qualificazione sul piano giuridico. Infatti, buona parte delle frodi che avvengono (anche) attraverso l'uso di tecnologie informatiche deve essere inquadrata alla luce della truffa tradizionale di cui all'art. 640 c.p., e non nella diversa fattispecie della frode informatica propriamente detta e prevista dall'art. 640-*ter* c.p.

Soltanto per fare un esempio: chi acquista un bene da un sito internet e si vede recapitato un bene del tutto diverso (e di minor valore) rispetto a quello descritto, subisce una truffa in senso classico. Non rileva, in altre parole, che sia stato tratto in inganno sulla rete. Chi, invece, effettua una operazione bancaria online pensando di operare sul sito del proprio istituto di credito, senza accorgersi di stare operando in realtà su un sito clonato verso il quale è stato indirizzato automaticamente da un *malware* che ha infettato il suo device, subisce il reato di cui all'art. 640-*ter* c.p. nel momento in cui il malfattore riesce a usare quelle credenziali per distrarre una somma di denaro dal suo conto corrente.

Considerata dunque la straordinaria entità del fenomeno, credo che sarebbe opportuno cogliere l'occasione offerta dal presente disegno di legge per ridisegnare l'impianto normativo a presidio dei diritti dei soggetti colpiti da fenomeni fraudolenti.

In particolare, potrebbe essere l'occasione per affrontare un problema rilevante sia sul piano teorico sia sul piano pratico.

Come dimostra in maniera inoppugnabile l'analisi della giurisprudenza in materia, è sempre più complesso – a causa dello sviluppo tecnologico e in particolare dell'impiego degli ultimi esiti dell'intelligenza artificiale – individuare chiari criterî di distinzione tra le fattispecie di cui all'art. 640 c.p. e all'art. 640-*ter*.

Rispetto all'art. 640, il 640-*ter* non richiede l'induzione in errore di un soggetto attraverso artifizi o raggiri. Dottrina e giurisprudenza, dopo una fase che ha fatto emergere orientamenti contrastanti, si sono poi indirizzate in maniera piuttosto decisa verso un'interpretazione che — data l'impossibilità di "trarre in inganno" una macchina che, per quanto "intelligente", non corrisponde ad un essere umano — non considera rilevante ai fini della configurabilità del reato la cooperazione del soggetto tratto in inganno. La frode informatica si caratterizzerebbe dunque rispetto alla truffa in quanto le condotte ad essa riferibili investono non un soggetto passivo, ma un sistema informatico.

Testo vigente	Nuova possibile formulazione
Articolo 615-*quater* Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici (L'articolo era originariamente rubricato «Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici». La rubrica è stata modificata dall'art. 19, comma 1, lett. c), l. 23 dicembre 2021, n. 238, che ha introdotto anche alcune modifiche al testo)	Articolo 615-*quater* Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici
«Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti, 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 due anni e con la multa sino a 5.164 euro».	«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 fino ad un anno e con la multa fino a euro 5.164».
Articolo 615-*quinquies* Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico.	Articolo 615-*quinquies* Detenzione, diffusione e installazione di apparecchiature, dispositivi o programmi informatici idonei all'accesso abusivo ad un sistema informatico o telematico.
«Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329».	«Chiunque, allo scopo di introdursi abusivamente in un sistema informatico o telematico, si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici è punito con la reclusione fino a due anni e con la multa fino a euro 10.329».

Tab. 2

Si tratterebbe pertanto di un reato finalizzato sempre all'ottenimento di un ingiusto profitto con altrui danno, che si concretizza tuttavia specificamente in una condotta illecita intrusiva o alterativa del sistema informatico o telematico (da ultimo si veda Cassazione penale, sez. II, 2 febbraio 2017, n. 9191).

Sta di fatto che la formulazione adottata dal legislatore risulta ambigua sotto diversi profili. La giurisprudenza si è trovata quindi più volte in gravi difficoltà, e un esame anche superficiale delle pronunce sul tema mette in evidenza come casi concreti praticamente identici siano stati a volte inquadrati nell'ambito dell'art. 640 e altre volte in quello dell'art. 640-*ter*. Basti citare la sentenza con cui il Tribunale di Roma (26 febbraio 2016, n. 2787) ha ravvisato la sussistenza del reato di frode informatica nel caso di un soggetto che aveva sottratto le credenziali di una carta di credito al fine di effettuare delle scommesse online, citando a conforto della propria decisione la «pacifica giurisprudenza della Suprema Corte di Cassazione» secondo cui «integra il reato di frode informatica ex art. 640-*ter* del Codice penale, la condotta di introduzione nel

sistema informatico delle Poste italiane mediante l'abusiva utilizzazione dei codici di accesso personale di un correntista e di trasferimento fraudolento, in proprio favore, di somme di denaro, depositate sul conto corrente del predetto». Tuttavia, in casi sostanzialmente identici si è invece sostenuta la sussistenza del reato di truffa, sulla scorta della considerazione che ad essere "raggirato" sembra il titolare della carta di credito più che il sistema informatico.

Ad aumentare ulteriormente la problematicità applicativa della disposizione di cui all'art. 640-*ter* sono i casi che riguardano la clonazione di carte di credito. Intorno a questi esiste un vero e proprio contrasto giurisprudenziale registrato dalla stessa Corte Cassazione (Cassazione penale, sez. II, 14 febbraio 2017, n. 8913), che ha preso atto della difficoltà di qualificare in maniera univoca l'utilizzo indebito di supporti magnetici clonati, potendo essere con validi motivi ricondotto tanto all'indebito utilizzo di carte di pagamento di cui all'art. 493-*ter*, quanto appunto all'art. 640-*ter*.

Pensiamo, infine, al caso emblematico del *phishing*. Questo termine, da un punto di vista giuridico, non è univocamente riferibile all'una o all'altra fattispecie. Mentre, infatti, varianti come lo *smishing* o il *whaling* ricadono nella quasi assoluta totalità dei casi nell'ambito applicativo del tradizionale reato di truffa, il *pharming* o il *tabnabbing* sostanziano condotte invece generalmente riconducibili alla frode informatica.

Allo stato attuale, dunque, la qualificazione giuridica di un atto di *phishing* richiede un esame dettagliato della concreta condotta tenuta dal *phisher*, che di caso in caso può sostanziarsi in forme assai differenti, diversamente sanzionabili, e che a volte rivelano l'impossibilità di una tutela efficace.

Il medesimo problema di inquadramento, infine, è attestato dalle difficoltà nella corretta qualificazione giuridica dei fatti da parte delle forze dell'ordine: numerosissime sono infatti le notizie di reato formulate in maniera non convincente.

In via generale, due sono le strade (e tre le soluzioni) che, mi pare, (potevano e possono) essere intraprese.

La via più semplice: lasciare intatte le formulazioni di cui agli artt. 640 e 640-*ter* del codice penale, inasprendo tuttavia le sanzioni riferibili alla frode informatica. Questa strada – ripeto, la più semplice – non risolverebbe però i problemi

Testo vigente	Testo emendato dalle Commissioni
Art. 640 c.p. Truffa	Art. 640 c.p. Truffa
Chiunque, con artifizi 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 51 euro a 1.032 euro. La pena è della reclusione da uno a cinque anni e della multa da 309 euro a 1.549 euro: 1) se il fatto è commesso a danno dello Stato o di un altro ente pubblico o dell'Unione europea o col pretesto di far esonerare taluno dal servizio militare; 2) se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'Autorità. 2-bis) se il fatto è commesso in presenza della circostanza di cui all'articolo 61, numero 5) . Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal capoverso precedente.	Chiunque, con artifizi 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 51 euro a 1.032 euro. La pena è della reclusione da uno a cinque anni e della multa da 309 euro a 1.549 euro: 1) se il fatto è commesso a danno dello Stato o di un altro ente pubblico o dell'Unione europea o col pretesto di far esonerare taluno dal servizio militare; 2) se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'Autorità. 2-bis) se il fatto è commesso in presenza della circostanza di cui all'articolo 61, numero 5) . 2-*ter*) se il fatto è commesso a distanza attraverso strumenti informatici o telematici idonei a ostacolare la propria o altrui identificazione; Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal secondo comma, a eccezione di quella di cui al numero 2-*ter*.

Tab. 3

di distinzione tra truffa e frode informatica già richiamati.

La versione inizialmente presentata alle Commissioni non prevedeva alcuna modifica delle due disposizioni in questione. Nella versione emendata, invece, viene proposta una modifica del solo art. 640 nel senso riportato in tab. 3.

Temo che, invece di risolvere il problema appena accennato, questa proposta emendata dalle Commissioni possa ulteriormente complicarlo. Questo perché inasprisce la sanzione della truffa 'classica' condotta tramite "strumenti informatici o telematici idonei a ostacolare la propria o altrui identificazione", aggiungendo così un ulteriore fattore di complessità in una materia di per sé già poco chiara. Ferma restando la formulazione dei due articoli – e confermando anche l'incertezza nella distinzione tra truffa e frode informatica – il testo emendato si limita a modificare verso l'alto le comminatorie edittali nel caso in cui il truffatore si serva di strumenti digitali per colpire a distanza. Ma, nella pratica, un caso di *smishing* (che usa come vettore gli sms invece dei messaggi di posta elettronica, sfruttando la minore diffidenza degli utenti nei confronti di una tecnologia avvertita come antiquata e pertanto meno pericolosa) potrebbe rientrare nella previsione di cui al nuovo art. 640 comma 2-*ter*? La risposta, a parere dello scrivente, è tutt'altro che certa. Viceversa: perché una condotta di *pharming* (con cui il truffatore adotta una tecnica di corruzione del Domain Name System, facendo sì che l'indirizzo correttamente digitato dall'utente non venga "risolto" come dovrebbe, ma conduca invece all'apertura di una diversa pagina gestita e controllata dal *phisher*), attuata attraverso "strumenti informatici idonei a ostacolare la propria o altrui identificazione" (come nodi TOR e simili), ricadendo nell'ambito dell'art. 640-*ter*, dovrebbe essere sanzionata in maniera più lieve rispetto al caso di una truffa tradizionale innescata tramite la medesima metodologia? Se l'intento del legislatore è quello di sanzionare in maniera più grave le frodi attuate tramite sistemi capaci di ostacolare l'identificazione del truffatore, pare irragionevole prevedere questo irrigidimento solo per la truffa e non anche per la frode informatica.

Imboccando, invece, la strada della "riforma", si potrebbero sviluppare due soluzioni alternative: una soluzione "di fusione" sarebbe quella di assorbire la frode informatica nella truffa, abrogando l'art. 640-*ter* e adottando una più articolata formulazione del primo comma dell'art. 640 (oltre alla conseguente risistemazione delle attuali aggravanti); in alternativa, si potrebbe adottare la soluzione "del caso aggravato", prevedendo la frode informatica come variante cibernetica del reato di truffa, sulla falsariga della proposta riguardante l'art. 629 (e come già avvenuto per esempio per l'art. 612-*bis*) (tab. 4).

Tutte queste soluzioni presentano vantaggi, svantaggi e conseguenze da ponderare attentamente.

A parere di chi scrive, quella "del caso aggravato" sembrerebbe la più convincente. Da una parte, risolverebbe il problema della distinzione tra truffa e frode informatica, che sarebbero ricondotte ad unità. Dall'altra, rispetto alla soluzione "di fusione", consentirebbe di mantenere una specificità (e una sanzione più grave) nel caso di truffa condotta tramite strumenti informatici (con un aumento di pena pienamente giustificato dalla loro natura subdola).

Nel *cyberspace* siamo tutti più vulnerabili. Per questo motivo, mi sembra una scelta comprensibile quella di aumentare le sanzioni a carico di chi impiega le tecnologie digitali per colpire i punti più deboli della società.

Tuttavia, come già ricordato, questa scelta di politica legislativa non può non essere accompagnata da una più ampia strategia di pedagogia digitale, capace di far penetrare nella cittadinanza l'idea che alcune pratiche di cyber-igiene sono ormai diventate indispensabili per mantenere la salute di quell'organismo complesso, e ancora fragile, che è la società digitale.

Testo vigente	Soluzione "di fusione"	Soluzione del "caso aggravato"
Art. 640 c.p. Truffa	Art. 640 c.p. Truffa	Art. 640 c.p. Truffa
Chiunque, con artifizi 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 51 euro a 1.032 euro. La pena è della reclusione da uno a cinque anni e della multa da 309 euro a 1.549 euro: 1) se il fatto è commesso a danno dello Stato o di un altro ente pubblico o dell'Unione europea o col pretesto di far esonerare taluno dal servizio militare; 2) se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'Autorità. 2-*bis*) se il fatto è commesso in presenza della circostanza di cui all'articolo 61, numero 5) . Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal capoverso precedente.	Chiunque, con artifizi o raggiri, inducendo taluno in errore, *ovvero alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti*, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da 51 euro a 1.032 euro. La pena è della reclusione da uno a cinque anni e della multa da 309 euro a 1.549 euro: 1) se il fatto è commesso a danno dello Stato o di un altro ente pubblico o dell'Unione europea o col pretesto di far esonerare taluno dal servizio militare; 2) se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'Autorità. 2-*bis*) se il fatto è commesso in presenza della circostanza di cui all'articolo 61, numero 5). Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal capoverso precedente.	Chiunque, con artifizi 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 51 euro a 1.032 euro. La pena è della reclusione da uno a cinque anni e della multa da 309 euro a 1.549 euro: 1) se il fatto è commesso a danno dello Stato o di un altro ente pubblico o dell'Unione europea o col pretesto di far esonerare taluno dal servizio militare; 2) se il fatto è commesso ingenerando nella persona offesa il timore di un pericolo immaginario o l'erroneo convincimento di dovere eseguire un ordine dell'Autorità. 2-*bis*) se il fatto è commesso in presenza della circostanza di cui all'articolo 61, numero 5) . *2-ter) se il fatto è commesso alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti.* *2-quater) se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale o è commesso con abuso della qualità di operatore del sistema.* *La pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti.* *Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze previste dal capoverso precedente.*

Tab. 4