Stefano Pietropaoli

Informatica criminale

Diritto e sicurezza nell'era digitale

Giappichelli

INTRODUZIONE

Il presente volume intende sollecitare una riflessione sulle molte ombre della rivoluzione digitale. Per sgombrare subito il passo da qualsiasi lettura "tecnofobica": non si tratta qui di negare in alcun modo le straordinarie potenzialità – le mille luci – con cui la digitalizzazione stupisce e abbaglia l'essere umano. Si tratta, invece, di invitare a una riflessione sui problemi che si annidano nel possibile uso scorretto, illecito o ingiusto di tali tecnologie, a partire dalla considerazione che ovunque ci sia luce non può non esserci anche una zona d'ombra.

Anche le tecnologie informatiche, come ogni altra tecnologia, sono astrattamente neutrali[1]. In altre parole, esattamente come un martello può essere adoperato tanto per piantare un chiodo cui appendere un quadro, quanto per fracassare la testa di un uomo, così, sul piano giuridico, gli strumenti informatici possono essere impiegati sia per esercitare un diritto sia per violarlo.

Maggiore è il potenziale di una certa tecnologia, superiori sono i vantaggi che essa offre e, allo stesso tempo, più gravi sono le conseguenze legate al suo cattivo uso. Il processo di progressiva datificazione delle nostre esistenze, combinato con gli stupefacenti sviluppi dell'intelligenza artificiale, mette in evidenza tutte le fragilità di questa nuova forma di vita.

Larga parte della popolazione mondiale è ormai stabilmente online. Chiunque abbia un dispositivo e una connessione può condividere dati e informazioni in maniera sostanzialmente istantanea con un insieme indeterminato di persone in qualsiasi luogo esse si trovino. Questa opportunità sta determinando un nuovo modo di vivere, proiettato sempre più radicalmente nella dimensione del cosiddetto *cyberspace*[2]. La nostra esistenza, in questo modo, viene

---

[1] Ciò è vero però soltanto fino a quando le tecnologie rimangono un mezzo per raggiungere un fine: tutt'altro problema – di cui si avverte drammaticamente la presenza – è rappresentato dal farsi queste tecnologie un fine in sé.

[2] Il cyberspazio è una dimensione cibernetica della realtà costituita da più livelli: livello fisico (*physical layer*), composto da dispositivi e reti di dati; livello logico (*logical layer*), costituito da istruzioni, protocolli e sistemi attraverso i quali le macchine interagiscono tra loro (come il TCP/IP e il DNS); livello delle informazioni (*information layer*), ovvero dei contenuti del mondo digitale come pagine web e contenuti multimediali, e distinguibile a sua volta in livello

sempre più massicciamente "datificata" [3], vale a dire trasformata in dati e tradotta nel linguaggio parlato dalle macchine. La nostra stessa identità, dunque, viene ridotta in codice binario, tanto che l'identità personale si fonde e si confonde ormai con l'identità digitale: non si tratta più di proiettare nella rete ciò che già siamo al di fuori di essa, ma ciò che siamo dentro la rete diventa determinante nella costruzione della nostra identità, per come la percepiscono gli altri e per come la percepiamo noi stessi. Chi siamo, in altre parole, lo dice – a noi e al resto del mondo – la rete.

Non esiste una realtà che non sia anche realtà virtuale, nel senso che ciò che viviamo fuori dalla rete può "informare" la nostra esistenza nella rete, e ciò che viviamo nella rete può determinare il nostro modo di vivere fuori dalla rete. Ciò che è virtuale è reale, e ciò che è reale è virtuale. Un qualsiasi evento concreto, dal più banale al più drammatico, può essere immediatamente datificato – filmato, fotografato, registrato, "protocollato" – e immesso nella rete, contribuendo a dare forma alla nostra identità. Questo già di per sé è sicuramente un problema, ma ancor più grave mi sembra che un evento virtuale possa riverberarsi nella vita concreta, influenzandola in maniera sempre più incisiva.

Qualche esempio può aiutare a mettere a fuoco il tema. Scatto un selfie che, dopo un addio al celibato, mi ritrae con una bottiglia di whisky vuota in mano e un'espressione chiaramente alterata in volto, lo condivido in rete con i miei "amici", lo affido alla rete (senza contesto), poi quella foto viene commentata, inoltrata, ricondivisa, contribuisce a ridefinire la mia identità nella rete, fino ad arrivare a un possibile datore che escluderà la mia candidatura a una certa posizione lavorativa. Oppure: ricevo un messaggio di posta elettronica da quella che sembra essere la mia banca che mi invita a compiere alcune operazioni di aggiornamento delle mie credenziali per l'*home banking*, seguo le istruzioni e inconsapevolmente consegno tutte le informazioni necessarie a effettuare un bonifico su una carta prepagata, col risultato di perdere una consistente somma di danaro. O, ancora, registro con il mio partner un video a carattere sessualmente esplicito che, dopo la fine della nostra relazione, viene inviato a una chat e poi inoltrato (con effetto "virale") su diversi social network, con una ricaduta pesantissima sulla mia vita concreta, sui miei rapporti personali, sul mio lavoro.

---

sintattico e livello semantico, rispettivamente per indicare le informazioni destinate all'uso da parte delle macchine (*syntactic layer*), e le informazioni destinate alla comprensione umana (*semantic layer*); livello degli utenti (*user layer*), definito dall'approccio umano nei confronti dei dispositivi informatici.

[3] Uso l'espressione "datificazione" per indicare un fenomeno più radicale rispetto alla mera "digitalizzazione". Digitalizzare un documento, per esempio, significa trasformarlo direttamente in una serie di bit leggibili da una macchina. Datificare quello stesso testo, invece, significa non soltanto digitalizzarlo, ma anche dotarlo di una ulteriore serie di dati – più precisamente, metadati – che aggiungono elementi informativi significativi.

Si innesca, in altre parole, nell'unica e irriducibile realtà, un processo circolare tra vita online e vita offline, o meglio si forma un nodo che non può più essere districato. Gli esempi richiamano casi assai diversi (e inquadrabili in maniera molto distante sul piano giuridico), ma il tema centrale è comune: il controllo dei dati che ci riguardano.

In questa prospettiva, esclusa la strada di un impossibile ritorno alla vita offline, non rimane che affrontare i rischi ai quali questo processo di datificazione ci espone inesorabilmente. L'esercizio e la tutela dei diritti passano oggi necessariamente dalla consapevolezza di questo fenomeno e dalla necessità di governarlo senza rimanerne schiacciati.

Proprio al fine di sollecitare la riflessione in tale direzione, questo volume tenta di proporre una galleria di ombre, certo non esaustiva ma che spero possa dar conto della complessità dell'impatto della rivoluzione digitale sul diritto e sui diritti.

Il Capitolo 1 è dedicato alle zone d'ombra più facilmente identificabili, grazie alla previsione nel nostro ordinamento giuridico di fattispecie criminose (i cosiddetti "reati necessariamente informatici") che le individuano con un sufficiente grado di precisione. Si passerà poi a esaminare una categoria – quella dei *cybercrimes* – dai contorni più sfumati e segnata da una notevolissima varietà di manifestazioni, in cui si esprime con assoluta evidenza la contiguità tra online e offline. Saranno poi oggetto di attenzione le ombre più oscure, sia per gravità sia per difficoltà di lettura, che riguardano la guerra – e in particolare la sua nuova manifestazione quale *cyberwar* – e quelle che tradizionalmente sono considerate le due massime figure dell'inimicizia: il pirata e il terrorista. Infine, dopo tante ombre, si tenterà di dare conto di qualche spiraglio di luce, sia sul piano strettamente giuridico – con l'informatica forense – sia sul più ampio campo della *cybersecurity*.

Alcuni di questi temi presentano gradi di notevole complessità, difficilmente affrontabili con la sintesi che un volume come questo necessariamente richiede. Sperando di riuscire a rendere la lettura meno faticosa, ho dunque cercato di limitare l'uso delle note a piè di pagina, riportando i soli riferimenti bibliografici essenziali alla fine di ogni capitolo.

Questo volume cerca di mettere a frutto l'esperienza didattica ormai ventennale dei corsi di insegnamento, volti ad affrontare da diversi punti di vista il problema del rapporto tra diritto e tecnologie informatiche, da me tenuti presso le Università degli Studi di Firenze e di Salerno e presso la Scuola Marescialli dell'Arma dei Carabinieri.

A tutti i miei studenti devo moltissimo per i continui stimoli e sollecitazioni ad approfondire alcuni degli argomenti trattati nelle prossime pagine. Uno speciale ringraziamento va a chi, tra loro, durante o alla fine del proprio percorso universitario ha voluto approfondire in maniera particolarmente seria lo studio di alcune tematiche, consentendomi di instaurare un dialogo per me pre-

ziosissimo: Angelo Abbate, Valeria Barone, Francesca Bianculli, Francesco Mattagli e Stefano Pellegrini.

Molti sono i debiti che ho contratto verso molti colleghi e colleghe, amici e amiche, con cui ho avuto l'opportunità di discutere sotto diverse prospettive alcuni dei temi che vengono affrontati nelle prossime pagine. Tra loro voglio ricordare almeno Fernando Llano Alonso, Raffaella Brighi, Roger Campione, Thomas Casadei, Stefano Dorigo, Fernanda Faini, Tommaso Gazzolo, Nicola Lettieri, Ettore Maria Lombardi, Erik Longo, Sandro Luce, Filippo Murino, Massimo Palazzo, Monica Palmirani, Michele Papa, Rosaria Pirosa, Silvia Salardi, Andrea Simoncini e Serena Vantin.

Sono grato a Giuliano Giappichelli per avermi offerto l'opportunità di una nuova collaborazione con una casa editrice che da oltre un secolo gioca un ruolo culturale insostituibile nel campo degli studi giuridici. Durante la stesura del testo ho potuto contare sullo straordinario supporto di Lucio San Marco, per affidarmi infine alla professionalità (e alla pazienza) di Francesca Leva e Federica Modina. A tutti loro voglio esprimere la mia riconoscenza.

A mio padre, Roberto Pietropaoli, va la mia più profonda gratitudine per essersi prestato – ancora una volta – alla puntuale revisione di un testo lontanissimo dai suoi principali interessi.

Questo libro è dedicato alle mie figlie, Bianca e Lucia, per me fari che squarciano le ombre dei momenti più bui.

CAPITOLO 1
REATI INFORMATICI

SOMMARIO: 1.1. I reati "necessariamente informatici" previsti dall'ordinamento giuridico italiano. – 1.2. La violazione del "domicilio informatico". – 1.2.1. L'accesso abusivo a sistema informatico o telematico (art. 615-*ter* c.p.). – 1.2.2. Detenzione e uso di mezzi idonei all'accesso abusivo (art. 615-*quater* c.p.). – 1.2.3. Detenzione e uso di mezzi idonei a danneggiare un sistema informatico (art. 615-*quinquies* c.p.). – 1.3. L'alterazione delle comunicazioni telematiche e informatiche. – 1.3.1. Intercettazione, impedimento o interruzione illecita di comunicazioni e uso dei relativi mezzi (artt. 617-*quater* e 617-*quinquies* c.p.). – 1.3.2. Falsificazione, alterazione o soppressione di comunicazioni informatiche (art. 617-*sexies* c.p.). – 1.4. Il danneggiamento di dati e sistemi informatici. – 1.4.1. Il danneggiamento di informazioni, dati e programmi informatici (artt. 635-*bis* e 635-*ter* c.p.). – 1.4.2. Il danneggiamento di sistemi informatici o telematici (artt. 635-*quater* e 635-*quinquies* c.p.). – 1.5. La frode informatica. – 1.5.1. La frode informatica (640-*ter* c.p.). – 1.5.2. Il *phishing*. – 1.5.3. Il *pharming*. – *Riferimenti bibliografici*.

1.1. *I reati "necessariamente informatici" previsti dall'ordinamento giuridico italiano*

Le "ombre" dello sviluppo tecnologico costituiscono una delle sfide più importanti per il diritto penale contemporaneo. Ciò anche a causa di uno dei pilastri della scienza penalistica, ovvero il principio – espresso all'art. 2 del nostro Codice penale e riconosciuto all'art. 25 della Costituzione – per il quale «*nessuno può essere punito per un fatto che, secondo la legge del tempo in cui fu commesso, non costituiva reato*». Com'è facile capire, la rivoluzione digitale ha infatti comportato, comporta, e comporterà l'emersione di nuove condotte immediatamente percepibili come illecite, e che tuttavia non possono essere sanzionate senza un'espressa previsione normativa: in altre parole, non sono punibili fino a quando non sono formalmente riconosciute come reato.

Considerato anche il divieto di interpretazione analogica che contraddistingue la legge penale (con la conseguente impossibilità per i giudici di estendere alla dimensione cibernetica la portata applicativa di reati offline già esi-

stenti)[1] il legislatore è dunque chiamato a intervenire non appena si profilino all'orizzonte fenomeni criminali di natura inconsueta, inserendo nuove figure di reato nell'ordinamento giuridico.

Diverse sono state le modalità con cui nei diversi paesi si è intervenuti a livello legislativo per fronteggiare questa emergenza. In alcuni casi (ad esempio negli Stati Uniti)[2] si è scelto un metodo per così dire "organico": in altre parole, i nuovi reati sono stati inseriti in atti normativi autonomi, "codici" *ad hoc* o "testi unici". In altri casi (come in Italia) il criterio scelto è stato invece "evolutivo": i nuovi reati sono stati inseriti in un corpus normativo già esistente – nel nostro caso, il Codice penale – che è stato quindi integrato con le nuove disposizioni incriminatrici.

Il fenomeno della criminalità informatica ha attirato l'attenzione della dottrina (statunitense *in primis*) già intorno al 1970, quando vennero pubblicati i primi studî riguardanti comportamenti illeciti attuati tramite tecnologie informatiche, come la manipolazione o il sabotaggio di computer. Tuttavia, occorre aspettare gli anni Ottanta del secolo scorso per assistere a una effettiva emersione di pratiche illecite legate all'uso di tecnologie informatiche e al conseguente interessamento della dottrina penalistica a questo tema. In quel periodo si verificarono infatti le prime azioni di *hacking*, e alcuni esperti di programmazione diedero avvio alla creazione (e alla diffusione) di *malware* (*malicious software*, *software* malevolo). Occorre peraltro notare che questa fase è stata caratterizzata da una lunga serie di azioni "dimostrative", in cui esperti di tecnologia agivano più per mettere alla prova i sistemi di sicurezza (e magari per denunciarne la debolezza) che per finalità criminose. Basti pensare al caso dei 414's di Milwaukee nel 1983, quando sei adolescenti violarono i sistemi del Los Alamos National Laboratory, del Memorial Sloan-Kettering Cancer Center e della Security Pacific Bank.

L'organizzazione internazionale che ha giocato il ruolo fondamentale nello stimolare la riflessione su questi nuovi fenomeni criminali è stata sicuramente il Consiglio d'Europa. Il 13 settembre 1989, con la raccomandazione 89/9 del Comitato Direttore per i Problemi Criminali (CDPC), veniva stilata la cosiddetta "lista minima": un elenco di fattispecie criminose che il Consiglio indicava ai Paesi membri come urgentemente bisognose di un riconoscimento giuridico. Più precisamente, la raccomandazione 89/9 proponeva l'introduzione in tutti i Paesi membri di alcuni reati quali la frode informatica, il falso informatico, il danneggiamento dei dati e dei programmi informatici, l'accesso abu-

[1] Solo per fare un esempio: non si può sanzionare una violazione del domicilio informatico in base all'art. 614 c.p., che è applicabile soltanto al domicilio inteso in senso tradizionale.

[2] Penso in particolare al *Counterfeit Access Device and Computer Fraud and Abuse Act* del 1984.

sivo, la riproduzione non autorizzata di *software*, il sabotaggio informatico. A questi si aggiungevano reati minori, che furono inseriti in una lista "facoltativa".

Il legislatore italiano ha accolto l'indicazione della raccomandazione 89/9 con la legge 23 dicembre 1993, n. 547, recante «Modificazioni ed integrazioni alle norme del Codice penale e del Codice di procedura penale in tema di criminalità informatica». Con questo atto sono state previste nell'ordinamento giuridico italiano alcune nuove figure criminose, introdotte dagli artt. 615-*ter*, 615-*quater* e 615-*quinquies*, 617-*quater*, 617-*quinquies* e 617-*sexies*, 635-*bis* e 640-*ter* c.p. Inoltre, la legge 547/1993 in alcuni casi ha riadattato, aggiornato o integrato in vario modo fattispecie penali già esistenti (artt. 392, 420, 491-*bis*, 616, 621 e 623-*bis* c.p.). Se è vero che anche prima del 1993 il legislatore era intervenuto sporadicamente sulla materia[3], è però solo con questo intervento normativo che i "reati informatici" sono entrati di fatto nell'ordinamento giuridico italiano.

Prima di passare all'esame di questi reati, mi sembra indispensabile chiarire una precisa scelta terminologica. Nel presente capitolo vengono trattati i soli "reati necessariamente informatici", ovverosia quei reati che non possono essere commessi se non attraverso l'utilizzo di tecnologie informatiche. Soltanto per fare un esempio: il reato di accesso abusivo a sistema informatico può essere commesso esclusivamente attraverso un dispositivo digitale, mentre così non è per reati quali lo *stalking* (il delitto di atti persecutorî), che possono essere perpetrati anche in maniera completamente offline e sono pertanto reati solo "occasionalmente informatici". Considerata, tuttavia, l'estrema frequenza con cui questi ultimi reati vengono commessi per il tramite di strumenti informatici, ho scelto di esaminarne le manifestazioni cibernetiche nel prossimo capitolo, raggruppandole sotto l'etichetta – certo non del tutto precisa ma, spero, efficace – di *cybercrimes*.

Nelle prossime pagine mi limiterò dunque a riportare quelli che mi sembrano gli elementi fondamentali di alcuni dei reati introdotti dalla legge 547/1993, anche alla luce dell'intervento di aggiornamento e integrazione da parte della legge 18 marzo 2008, n. 48, con cui l'Italia ha ratificato un accordo internazionale, anch'esso promosso dal Consiglio d'Europa: la "Convenzione sulla criminalità informatica" firmata a Budapest il 23 novembre 2001.

Nel tentativo di rendere maggiormente comprensibili le disposizioni normative qui esaminate, ho ritenuto opportuno proporne una analisi schematica affiancata, laddove possibile, da esempi ricavati dalla giurisprudenza sul tema.

---

[3] Ricordo, ad esempio, la legge 18 maggio 1978, n. 191, che prevedendo l'introduzione nel Codice penale dell'art. 420 sanzionava l'attentato ad impianti di pubblica utilità, ivi compresi gli impianti di elaborazione di dati.

1.2. *La violazione del "domicilio informatico"*

1.2.1. *L'accesso abusivo a sistema informatico o telematico (art. 615-*ter *c.p.)*

Una delle più importanti novità introdotte dalla legge 547/1993 è sicuramente il reato di accesso abusivo ad un sistema informatico o telematico di cui all'art. 615-*ter* c.p. Già considerando la sua collocazione, immediatamente successiva alla violazione di domicilio[4], si intuisce come la disposizione sia stata costruita come una "violazione del domicilio informatico".

La lettura del comma 1 dell'art. 615-*ter*, il cui tenore letterale è assolutamente prossimo a quello dell'art. 614, è sufficiente a confermare questa ipotesi: «*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*». Tanto la posizione dell'articolo all'interno del Codice quanto la costruzione sintattica e semantica della norma consentono dunque di considerare l'art. 615-*ter* come un delitto contro l'inviolabilità di quel «domicilio informatico» che, secondo la dottrina dominante, è rappresentato dai sistemi informatici intesi come espansione ideale del bene protetto dall'art. 14 della Costituzione.

L'art. 615-*ter* prevede un reato di mera condotta: perché si possa configurare il reato non è quindi necessario che si verifichi un determinato evento (per esempio, la sottrazione di contenuto informativo), ma è sufficiente che sia accertata una delle condotte previste dalla disposizione. Le forme tipiche in cui questa condotta può esprimersi sono due: l'introduzione abusiva in un sistema informatico protetto da misure di sicurezza (ad esempio una password)[5] oppure la permanenza in esso senza l'autorizzazione dell'avente diritto.

Per inquadrare la questione nella maniera più efficace può essere di aiuto il ricorso all'immagine della violazione di domicilio. In primo luogo, commette il reato previsto dall'art. 615-*ter* chi entra in un domicilio informatico – un device personale, certo, ma anche un semplice account di qualsiasi servizio digitale[6] – varcandone senza autorizzazione la porta di ingresso: una porta di cui potreb-

---

[4] Art. 614 c.p.: «*Chiunque s'introduce nell'abitazione altrui, o in altro luogo di privata dimora, o nelle appartenenze di essi, contro la volontà espressa o tacita di chi ha il diritto di escluderlo, ovvero vi s'introduce clandestinamente o con l'inganno, è punito con la reclusione da uno a quattro anni*»).

[5] Si noti che se il sistema non è protetto da una misura di sicurezza, manca un elemento essenziale della fattispecie e pertanto non è configurabile il reato di accesso abusivo.

[6] Commette dunque il reato di cui all'art. 615-*ter* c.p. chi, per esempio, accede alla casella di posta elettronica altrui senza il consenso del titolare. Un account di posta è, difatti, un domicilio informatico protetto da una password che esprime la volontà dell'utente di farne uno spazio a sé riservato (così Cass. pen., sez. V, 28 ottobre 2015, n. 13057).

be aver forzato la serratura (un *hacker* capace di *crackare* la password di accesso), o della quale si è procurato una copia delle chiavi (magari sbirciando il titolare mentre digitava ID e codice di login), o che addirittura potrebbe aver trovato spalancata (come nel caso di una sessione di *webmail* lasciata aperta su un device, senza cioè effettuare il *logout*).

In secondo luogo, commette reato anche chi, pur essendosi introdotto lecitamente in un domicilio informatico, vi si mantiene contro la volontà del titolare (espressa o tacita). In tale ipotesi viene sanzionato non tanto l'accesso, quanto l'uso del domicilio informatico, come nel caso di chi, chiamato a controllare la funzionalità di un certo programma informatico, si avvalga della originaria autorizzazione del titolare per poi copiare, per fini esclusivamente personali, i dati inseriti in quell'applicativo (così già Cass. pen., sez. V, 7 novembre 2000, n. 12732, Zara).

Mi sembra particolarmente importante sottolineare come il reato sia configurabile anche nel caso in cui il soggetto sia abilitato ad accedere al sistema – di cui, dunque, detiene legittimamente le chiavi di accesso – e tuttavia violi le prescrizioni impartite dal titolare per delimitarne l'accesso (orientamento giurisprudenziale, questo, ormai consolidato, e che trova la più puntuale definizione in Cass. pen., sez. un., 27 ottobre 2011, n. 4694). Per esempio, un appartenente ad una forza di polizia, legittimamente in possesso delle credenziali per accedere al sistema informatico Banca Dati SDI, commette il reato di accesso abusivo a sistema informatico o telematico qualora effettui una ricerca con tale strumento per finalità estranee a quelle istituzionali (e, in particolare, previste dall'art. 6 della legge 121/1981). Allo stesso modo, integra il reato la condotta del dipendente di Equitalia che accede al sistema informatico della riscossione per accertare la posizione debitoria di un proprio congiunto (Corte Appello Lecce, 14 febbraio 2022, n. 1803), oppure il dipendente dell'Agenzia delle Entrate che si introduce nel sistema informatico dell'Anagrafe Tributaria ispezionando i nominativi di alcuni contribuenti, non per motivi di servizio, ma per la compilazione delle loro dichiarazioni dei redditi (Tribunale di Vicenza, 19 marzo 2021, n. 209).

Per quanto riguarda l'elemento soggettivo, l'art. 615-*ter* richiede il dolo generico: ai fini della sussistenza del reato non rilevano, dunque, gli scopi e le finalità che abbiano motivato l'ingresso o la permanenza non autorizzata nel sistema, ma rileva la sola volontà di tenere una determinata condotta.

Nei casi indicati al comma 1, il delitto è punibile a querela della persona offesa. Si procede invece d'ufficio nei più gravi casi previsti al comma 2, che prevede la reclusione da uno a cinque anni: «1*) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della*

qualità di operatore del sistema; 2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato; 3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti».

Il legislatore ha inoltre posto particolare attenzione ai casi in cui oggetto della condotta illecita siano sistemi informatici di interesse militare, oppure relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico. In tali casi la pena è aumentata: rispettivamente, è prevista la reclusione da uno a cinque anni per i casi previsti dal comma 1 e da tre a otto anni per quelli indicati dal comma 2.

1.2.2. *Detenzione e uso di mezzi idonei all'accesso abusivo (art. 615-*quater *c.p.)*

Oltre a stabilire l'illiceità dell'accesso abusivo a un sistema informatico, il nostro ordinamento sanziona anche alcune condotte prodromiche alla vera e propria introduzione in un domicilio informatico.

In questo senso, l'art. 615-*quater* prevede il reato di «Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici»[7]: «*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*».

Riprendendo l'immagine della violazione di domicilio: si sanziona non soltanto chi si introduce nella dimora di qualcuno senza autorizzazione, ma anche chi si procura grimaldelli o strumenti analoghi (dispositivi *hardware* o *software*) atti a forzare la porta di ingresso, oppure diffonde copie delle chiavi di accesso (le password). Il legislatore ha voluto così anticipare la soglia della punibilità rispetto al momento dell'effettivo conseguimento di un profitto, concependo la fattispecie quale reato di pericolo e non già quale illecito di danno. Come per il 615-*ter*, la disposizione punisce la mera condotta, senza riguardo dunque all'effettivo verificarsi di un determinato evento (il reato si rea-

[7] 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), legge 23 dicembre 2021, n. 238, che ha introdotto anche alcune modifiche al testo.

lizza anche se non si concretizza un danno). Per quanto riguarda l'elemento soggettivo, invece, il 615-*quater* richiede il dolo specifico: il reato sussiste, dunque, solo in presenza della precisa volontà di procurare a sé o altri un profitto oppure di arrecare ad altri un danno (anche se questo, ripetiamo, non si dovesse concretizzare).

Importante è sottolineare che i reati di cui agli artt. 615-*ter* e 615-*quater* non possono "concorrere" tra loro se contestati nel medesimo contesto spazio-temporale o e in danno dello stesso soggetto. Ciò in quanto il reato di cui al 615-*quater* è necessario antecedente dell'accesso abusivo. Le due fattispecie si pongono in stretta connessione: tutelano entrambe il medesimo bene giuridico – il domicilio informatico – passando da condotte meno invasive a interventi più penetranti, che necessariamente presuppongono le prime (Cass. pen., sez. II, 14 gennaio 2019, n. 21987).

Esempio di una condotta punibile *ex* art. 615-*quater* è quella di chi comunica, dietro compenso, le credenziali di accesso ad account personali abusivamente scaricate da un database. Qualora si tratti invece di codici di carte di credito, che il soggetto intende inserire in supporti "clonati", l'inquadramento diventa più complesso. Nel caso in cui si realizzi la finalità di prelevare denaro contante attraverso il sistema bancomat, il reato in oggetto può infatti essere assorbito nella fattispecie più gravemente sanzionata dall'art. 55, comma 9 del d.lgs. 231/2007 (e successivamente confluito nell'art. 493-*ter* c.p.) in tema di utilizzazione illecita di carte di credito o di pagamento (Cass. pen., sez. II, 3 ottobre 2013, n. 47021).

Per quanto riguarda la detenzione o diffusione abusiva di smart card "pirata" (schede informatiche che consentono di visualizzare programmi televisivi criptati) la giurisprudenza si è orientata verso la non applicabilità dell'art. 615-*quater*, inquadrando invece l'ipotesi alla luce dell'art. 171-*octies* della legge 22 aprile 1941, n. 633 a tutela del diritto di autore. Analogamente, in riferimento all'uso di apparati (cosiddetti "pezzotti") atti alla decodificazione di trasmissioni via IPTV in elusione delle misure tecnologiche di protezione attuate dall'emittente, al fine di sottrarsi al pagamento del canone dovuto per l'accesso ai programmi, la Suprema Corte ha affermato la configurabilità del reato previsto dall'art. 171-*octies* della legge 633/1941 (Cass. pen., sez. III, 30 gennaio 2017, n. 46443).

1.2.3. *Detenzione e uso di mezzi idonei a danneggiare un sistema informatico (art. 615-*quinquies *c.p.)*

L'art. 615-*quinquies* c.p., rubricato «Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a dan-

neggiare o interrompere un sistema informatico o telematico»[8], dispone che «*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*».

Il testo originale è stato modificato prima con la legge 18 marzo 2008, n. 48 e poi con la legge 23 dicembre 2021, n. 238. Nella versione del 1993 il reato si configurava esclusivamente mediante la diffusione di prodotti informatici dannosi, mentre la disposizione vigente punisce la creazione, detenzione, diffusione e installazione sia di componenti *hardware* in grado di danneggiare sistemi informatici e telematici, sia di programmi applicativi rientranti sotto la categoria di *malware*. Rientrano in questa seconda tipologia i virus informatici propriamente detti, i *worms*, i *trojan horses* e moltissimi altri tipi di applicativi malevoli.

Per quanto riguarda l'elemento soggettivo, l'art. 615-*quinquies* prevede un dolo specifico: il fatto è punito soltanto se commesso col preciso scopo di danneggiare illecitamente un sistema, 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.

Rientra nella fattispecie punita dall'art. 615-*quinquies*, per esempio, la condotta di chi manipoli un *software* in maniera tale che compia azioni non volute dall'utente, contro la volontà dell'utilizzatore e con lo scopo di danneggiarne il sistema. Ricordo a questo proposito la sentenza del Tribunale di Bologna, sez. I, 22 dicembre 2005, n. 1823, che può essere considerata la prima pronuncia su di un *worm* italiano. Tale era infatti Vierika, un *malware* programmato in Visual Basic Script che veniva allegato a messaggi di posta e, se eseguito, interveniva sulla configurazione del sistema operativo Windows, riducendo al minimo il livello di protezione del browser Internet Explorer e inserendovi una *home page* predefinita diversa da quella preimpostata oppure scelta dall'utente. Nel momento in cui l'utente si collegava ad internet e apriva il *browser*, veniva lanciato automaticamente uno *script* che – sfruttando le falle create in prima battuta – creava un file che veniva inviato agli indirizzi e-mail contenuti nella rubrica del *client* di posta elettronica del sistema operativo infettato.

[8] Anche in questo caso, la rubrica è stata modificata dall'art. 19, comma 1, lett. c), legge 23 dicembre 2021, n. 238, che ha pure modificato il testo dell'articolo, sul quale era già intervenuta la legge 38/2008.

1.3. *L'alterazione delle comunicazioni telematiche e informatiche*

1.3.1. *Intercettazione, impedimento o interruzione illecita di comunicazioni e uso dei relativi mezzi (artt. 617-*quater *e 617-*quinquies *c.p.)*

La tutela delle comunicazioni telematiche e informatiche è stata formulata dalla legge 547/1993 in maniera assolutamente speculare rispetto alle previsioni introdotte per le comunicazioni e conversazioni telefoniche e telegrafiche dalla legge 8 aprile 1974, n. 98, che ha novellato l'art. 617 e inserito nel Codice penale gli artt. 617-*bis* e 617-*ter*.

L'art. 617-*quater* prevede il reato di «Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche»: «*1. Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da un anno e sei mesi a cinque anni. 2. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma. 3. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa. 4. Tuttavia si procede d'ufficio e la pena è della reclusione da tre a otto anni se il fatto è commesso: 1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità; 2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema; 3) da chi esercita anche abusivamente la professione di investigatore privato*».

L'articolo tutela, dunque, le comunicazioni relative ad un sistema oppure intercorrenti tra più sistemi. La condotta punita si sostanzia nella intercettazione fraudolenta di dette comunicazioni, oppure nel loro impedimento o interruzione. Per quanto riguarda l'elemento soggettivo, è richiesto il dolo generico.

Quale esempio del reato di cui all'art. 617-*quater* (in una delle sue forme aggravate), si può individuare la condotta dell'amministratore di sistema che predisponga un *software* appositamente finalizzato alla intercettazione delle comunicazioni tra gli utenti di un servizio di posta elettronica (Cass. pen., sez. V, 6 luglio 2007, n. 31135).

Il legislatore ha inteso anticipare la tutela prevedendo all'art. 617-*quinquies* il reato di «Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche»[9]: «*1. Chiunque, fuori dai casi consentiti dalla legge,*

[9] Rubrica introdotta dall'art. 19, comma 6, lett. b), legge 23 dicembre 2021, n. 238. Il testo

al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle, si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni. 2. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater».

Rispetto al caso previsto dall'art. 617-*quater*, la condotta qui si limita alla installazione degli apparecchi atti a intercettare, impedire o interrompere le comunicazioni relative a un sistema o tra più sistemi. Il legislatore ha voluto dunque punire anche la mera installazione di tali apparecchi. Qualora la condotta iniziale si sviluppi nella intercettazione di cui all'art. 617-*quater*, non si avrebbe concorso tra i due reati, ma assorbimento nella fattispecie più grave (così Cass. pen., sez. V, 18 dicembre 2015, n. 4059).

Per esempio, integra il reato di cui all'art. 617-*quinquies* c.p. la condotta di chi, al posto del pannello originario, installi su uno sportello bancomat un'apparecchiatura capace di memorizzare i codici digitati, quando non vi sia prova certa dell'intercettazione di almeno un codice identificativo (Cass. pen., sez. V, 1° febbraio 2016, n. 23604). Ai fini di una maggiore esemplificazione, pensiamo al caso in cui venga installato uno *skimmer* che consenta di intercettare i dati della banda magnetica della carta di credito utilizzata presso uno sportello bancomat, mentre una microtelecamera nascosta registra la digitazione del codice segreto sulla tastiera. Qualora tali dati, astrattamente idonei a ottenere carte clonate abilitate al pagamento o al prelievo di denaro contante, non vengano utilizzati, si configura il reato di cui all'art. 617-*quinquies* c.p.; in caso contrario, si avrà il reato *ex* art. 617-*quater* (Tribunale di Napoli, sez. V, 10 maggio 2012, n. 6531).

1.3.2. *Falsificazione, alterazione o soppressione di comunicazioni informatiche (art. 617-*sexies *c.p.)*

L'art. 617-*sexies* disciplina invece la «Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche». Il testo della norma è il seguente: «*1. Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di*

precedente era «Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche».

*taluna delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro anni. 2. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-*quater*. 3. Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa*».

Quanto all'elemento soggettivo, il testo indica chiaramente il dolo specifico (procurare a sé o ad altri un vantaggio o cagionare ad altri un danno). Il delitto qui sanzionato ha delle evidenti affinità con il falso materiale, concernente in questo caso un documento informatico. La fattispecie qui configurata è tuttavia diversa da quella che risulta dal combinato disposto dagli artt. 485, 490 e 491-*bis* c.p., in quanto disciplina il caso speciale di un documento oggetto di comunicazione.

Per fare un esempio: rientra nell'ambito applicativo dell'art. 617-*sexies* il caso della falsificazione della notifica di avvenuta lettura di una e-mail di convocazione per una procedura concorsuale indetta da un ente locale (condotta tenuta al fine di evitare la partecipazione al concorso di un determinato candidato).

Come vedremo meglio più avanti, questo reato è configurabile in una delle tipiche condotte con cui si realizza il c.d. *phishing*, e in particolare – per ricordare un fenomeno oggi estremamente frequente – nella falsificazione di comunicazioni di istituti di credito che mirano a carpire i codici (user ID e password) relativi a servizi finanziari on line.

1.4. *Il danneggiamento di dati e sistemi informatici*

1.4.1. *Il danneggiamento di informazioni, dati e programmi informatici (artt. 635-*bis *e 635-*ter *c.p.)*

L'art. 635-*bis*, il cui testo originale è stato modificato dalla legge 48/2008, è rubricato «Danneggiamento di informazioni, dati e programmi informatici» e dispone che «*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*». Il comma 2 (novellato dall'art. 2, d.lgs. 15 gennaio 2016, n. 7) aggiunge che «*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*».

Il bene tutelato coincide, in questo caso, non col sistema informatico (tutelato invece *ex* art. 635-*quater*), ma con le informazioni, i dati e i programmi ivi

contenuti. L'elemento materiale è costituito dal mero danneggiamento del sistema, da una condotta dunque finalizzata ad impedire che il sistema funzioni. Diversamente dai casi aggravati contemplati negli articoli successivi (635-*ter*, quater e quinquies), l'art. 635-*bis* dispone la procedibilità a querela della persona offesa, sostituita da quella d'ufficio in caso di ricorrenza delle circostanze aggravanti di cui al comma 2.

Per quanto riguarda la formulazione dell'articolo, mi preme sottolineare un punto che mi pare di particolare interesse a proposito del rapporto tra evoluzione tecnologica e interpretazione normativa. Nel testo si fa riferimento tanto alla distruzione quanto alla cancellazione di dati. In un altro contesto i due termini potrebbero indicare due condotte sostanzialmente indistinguibili l'una dall'altra. In riferimento ai dati informatici, invece, la cancellazione è distinta dalla distruzione in quanto quest'ultima indica un'eliminazione definitiva dei dati. Il legislatore ha voluto dunque punire, inserendo espressamente l'ipotesi della cancellazione, anche la condotta che comporta la sola perdita temporanea di dati che possono essere in seguito ripristinati. Da ciò deriva la configurabilità del reato di danneggiamento informatico anche in caso di manomissione o alterazione che cagioni un danno non definitivo e dunque rimediabile (in questo senso, *ex plurimis*, Cass. pen., sez. V, 18 novembre 2011, n. 8555).

L'art. 635-*ter*, come anticipato, prevede un caso aggravato rispetto al precedente: il «Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità». La disposizione normativa recita: «*1. Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni. 2. Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto anni. 3. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata*».

La norma, introdotta dalla legge 48/2008 (il comma 3 è stato novellato dall'art. 2, d.lgs. 15 gennaio 2016, n. 7) tutela l'ordine pubblico rispetto ad atti diretti contro sistemi informatici di pubblica utilità e contro dati, informazioni e programmi in essi contenuti. Il reato è perseguibile d'ufficio e, per quanto riguarda l'elemento soggettivo, richiede il dolo generico.

Il bene che viene qui difeso è l'interesse collettivo all'integrità di dati di rilievo pubblico. In quanto tali, ad essi viene accordata una tutela rafforzata rispetto a quella di cui all'art. 635-*bis*. Infatti, non viene punito soltanto chi distrugge, cancella o altera dati, ma anche chi commette un fatto diretto a di-

struggere, cancellare o alterare dati. In altre parole, si ha qui un'anticipazione della punibilità. Il comma 2 stabilisce invece una pena più severa nel caso si verifichi l'evento dannoso.

La pena è aumentata nel caso in cui ricorrano le aggravanti di cui all'ultimo comma, e dunque se il fatto viene commesso con violenza alla persona o con minaccia ovvero sia realizzato con abuso della qualità di operatore del sistema.

1.4.2. *Il danneggiamento di sistemi informatici o telematici (artt. 635-*quater *e 635-*quinquies *c.p.)*

Il «Danneggiamento di sistemi informatici o telematici» di cui all'art. 635-*quater* c.p. costituisce una autonoma fattispecie costruita a partire dall'art. 635-*bis*. La disposizione così recita: «*1. Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-*bis*, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni. 2. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata*».

Anche in questo caso la norma è stata introdotta dalla legge 48/2008, mentre il comma 2 è stato novellato dall'art. 2 della legge 7/2016. Procedibile d'ufficio, per quanto riguarda l'elemento soggettivo il reato sussiste con il dolo generico.

Il delitto che viene qui configurato è inquadrabile come reato a forma vincolata, il cui obiettivo è la distruzione o (più realisticamente) il danneggiamento non di dati e informazioni ma di sistemi informatici nel loro complesso. Come ha chiarito la Cassazione (Cass. pen., sez. II, 14 dicembre 2011, n. 9870), l'oggetto del delitto è infatti costituito dal complesso di apparecchiature interconnesse o collegate tra loro, in cui una o più di esse effettui il trattamento automatico di dati mediante un programma (nella specie, il sistema di videosorveglianza di un ufficio giudiziario, composto da apparati di videoregistrazione e da un componente dedicato al trattamento delle immagini e alla loro memorizzazione).

È interessante notare come il legislatore abbia dato "copertura" tanto ai casi in cui un sistema viene danneggiato o reso inservibile – ad esempio con un virus – quanto i casi in cui di questi venga ostacolato gravemente il funzionamento. La formulazione adottata può quindi punire anche un attacco attuato per mezzo di una botnet, ad esempio un DDoS (*Distributed Denial of Service*) capace di far esaurire le risorse di un sistema a causa di un numero di richieste talmente elevato da renderlo incapace di erogare i servizi richiesti.

Il reato previsto all'art. 635-*quinquies*, rubricato «Danneggiamento di sistemi informatici o telematici di pubblica utilità» rappresenta, ovviamente, un'ipotesi aggravata rispetto al reato *ex* art. 635-*quater*, rispetto al quale assicura, di conseguenza, una tutela rafforzata che si manifesta nella punibilità anticipata alla fase del tentativo. Il testo recita: «*1. Se il fatto di cui all'articolo 635-*quater *è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni. 2. Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto anni. 3. Se il fatto è commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema, la pena è aumentata*».

La condotta consiste nel compimento di atti diretti al danneggiamento di un sistema informatico o telematico di pubblica utilità. Anche in questo caso si ha un reato a consumazione anticipata, che viene perfezionato con il solo compimento dell'azione. Per quanto riguarda l'elemento soggettivo, è richiesto il dolo generico.

Analogamente a quanto visto a proposito dell'art. 635-*ter*, il comma 2 sanziona il caso in cui si verifichi l'effetto lesivo; un aggravamento della pena è disposto dal comma 3 qualora il fatto sia commesso con violenza alla persona o con minaccia ovvero con abuso della qualità di operatore del sistema.

1.5. *La frode informatica*

1.5.1. *La frode informatica (640-*ter *c.p.)*

Con l'art. 640-*ter* giungiamo alla disposizione che, tra quelle introdotte dalla legge 547/1993 o dalla legge 48/2008, riveste forse il maggiore interesse sia sul piano dottrinale. sia su quello applicativo. A quest'ultimo proposito, le statistiche mostrano un rapidissimo aumento delle denunce riferibili a operazioni fraudolente, di varia natura, avvenute in rete o per mezzo della rete [10]. È tuttavia opportuno sottolineare che il fenomeno comunemente indicato come "truffe online" sia estremamente variegato e di non semplice qualificazione sul piano giuridico. Infatti, buona parte delle frodi che avvengono (anche) attraverso

[10] Secondo i dati ISTAT, il numero di delitti denunciati dalle forze di polizia all'autorità giudiziaria in materia di truffe e frodi informatiche è passato dai 150.000 del 2016 a quasi 250.000 nel 2020.

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 da un *malware* che ha infettato il suo dispositivo, 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.

La «Frode informatica» di cui all'art. 640-*ter* viene, infatti, disciplinata dal nostro ordinamento come segue: «*1. Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da 51 euro a 1.032 euro. […]*»[11].

La lettura della disposizione indica chiaramente due condotte alternative. Da una parte, si ha l'alterazione del funzionamento di un sistema (per esempio, attraverso un virus o un altro *malware*). Dall'altra, si ha invece l'intervento su dati, informazioni o programmi contenuti in un sistema. In questo secondo caso è da sottolineare come l'intervento debba essere «senza diritto»: questa espressione comprende sia l'assenza del consenso del titolare dei dati, sia ogni modalità non consentita da norme giuridiche.

Perché il reato possa essere configurato, occorre che si verifichi l'ingiusto profitto con altrui danno: senza questo elemento potranno ravvisarsi gli estremi di altri reati, ma non si avrà frode informatica (e neppure una truffa in senso classico).

Uno dei problemi interpretativi sorti a proposito dell'art. 640-*ter*, come già accennato, riguarda la sua correlazione con il reato di truffa. 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

[11] I riferimenti al trasferimento di denaro, di valore monetario o di valuta virtuale sono stati inseriti dall'art. 2, comma 1, lett. c), d.lgs. 8 novembre 2021, n. 184.

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. 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 Cass. pen., sez. II, 2 febbraio 2017, n. 9191).

Sta di fatto che la formulazione adottata dal legislatore risulta ancora ambigua sotto alcuni 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*.

Per riflettere sulla difficoltà di distinguere tra truffa e frode informatica 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*». 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 (già ricordati in riferimento all'art. 615-*quater*) che riguardano la clonazione di carte di credito. Intorno a questi esiste un vero e proprio contrasto giurisprudenziale registrato dalla stessa Corte Cassazione (Cass. pen., 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*.

Per completezza, ricordo anche che l'art. 640-*quinquies* sanziona la particolare frode informatica perpetrata da un soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato.