

ROMANCE SCAM

La truffa affettiva online

Come nasce, in quali condotte si cade, come difendersi

Avv. Gianluca Giammatteo

PATROCINANTE IN CASSAZIONE — FORO DI ISERNIA

WWW.GIAMMATTEO.IT

Romance scam. La truffa affettiva online.

Il fenomeno, le condotte in cui la vittima può incappare e il quadro normativo per difendersi e recuperare.

Autore: Avv. Gianluca Giammatteo, del Foro di Isernia, Patrocinante in Cassazione.

Edizione a cura dello Studio Legale Giammatteo — Via Nicandro Iosso n. 6, 86079 Venafro (IS).

Testo aggiornato al mese di luglio 2026.

L'opera ha finalità informativa e formativa. Non costituisce parere legale, non instaura alcun rapporto professionale e non sostituisce l'esame del caso concreto. Il testo richiama la sola normativa vigente, con esclusione dei riferimenti giurisprudenziali; le disposizioni citate sono aggiornate alla data indicata e vanno verificate nella loro versione in vigore prima di ogni utilizzo in atti giudiziari. Si rinvia alla nota sulle fonti posta in chiusura.

© Studio Legale Giammatteo. Tutti i diritti riservati. È vietata la riproduzione, anche parziale, senza autorizzazione scritta.

Indice

Presentazione	5
PARTE PRIMA — IL FENOMENO	7
I. Che cos'è il romance scam	8
II. Come nasce e come si sviluppa	10
III. Le forme che assume oggi	11
PARTE SECONDA — LE CONDOTTE IN CUI SI CADE	12
IV. L'invio di denaro	13
V. L'«investimento» su piattaforme fittizie	14
VI. Le criptovalute e i wallet	15
VII. La vittima come «money mule»	16
VIII. Le immagini intime e la sextortion	17
IX. I dati, l'identità e gli accessi	18
X. La seconda ondata: la truffa del recupero	19
PARTE TERZA — IL QUADRO NORMATIVO	20
XI. I reati subiti dalla vittima	21
XII. I rischi penali della vittima	22
XIII. La tutela dei dati personali	23
XIV. Cripto-attività e antiriciclaggio	24
XV. I profili civili	25
PARTE QUARTA — COSA FARE	26
XVI. Denuncia e querela	27
XVII. Congelamento, sequestro e confisca	28
XVIII. Il recupero delle somme	29

XIX. Prevenzione e segnali d'allarme	30
L'autore	31
Nota e fonti normative	32

Presentazione

Chi entra in studio dopo una truffa affettiva porta con sé, quasi sempre, due ferite che non coincidono. La prima è economica e si misura in denaro: bonifici, ricariche, versamenti su piattaforme mai esistite. La seconda è personale e non si misura affatto: è la scoperta di aver dato fiducia, tempo e affetto a qualcuno che non c'era. Il romance scam colpisce insieme il patrimonio e la persona, e chiedere aiuto costa spesso più fatica per la vergogna che per il danno.

Questa guida nasce da un'esigenza pratica. Il romance scam non è un evento unico ma un percorso: comincia con una relazione costruita a tavolino e prosegue, di richiesta in richiesta, verso condotte sempre più impegnative. La vittima non si limita a «perdere dei soldi»: viene indotta a investire su false piattaforme, ad aprire conti e wallet, a ricevere e ritrasferire il denaro di altri, a condividere immagini intime, a consegnare documenti e credenziali. Alcune di queste condotte la espongono, oltre che al danno, a un rischio penale proprio, del quale quasi mai è consapevole. E quando il primo raggiro finisce, se ne affaccia spesso un secondo, la truffa del recupero, che promette di restituire il maltolto e produce soltanto un'ulteriore perdita.

Il testo segue questo percorso. La prima parte descrive il fenomeno e le sue fasi. La seconda passa in rassegna, una per una, le condotte in cui la vittima può incappare, così che ciascuno possa riconoscere la propria posizione. La terza inquadra la materia sul piano del diritto: i reati subiti, i rischi penali che la vittima può correre, la tutela dei dati personali, la disciplina delle cripto-attività e dell'antiriciclaggio, i rimedi civili. La quarta indica cosa fare in concreto: denuncia e querela, con i loro tempi; il congelamento, il sequestro e la confisca, anche oltre confine; il recupero delle somme e la costituzione di parte civile; la prevenzione.

Una scelta di metodo. Il testo richiama la sola normativa, con indicazione puntuale degli articoli, e non riporta pronunce giurisprudenziali. La ragione è duplice: offrire un riferimento stabile, che non invecchi con il mutare degli orientamenti, e restituire al lettore la struttura delle norme applicabili, non l'esito del singolo caso, che dipende sempre dai fatti. Le disposizioni citate sono aggiornate a luglio 2026 e vanno comunque verificate nella versione vigente prima di ogni impiego in un atto.

Un'ultima considerazione, la più importante. Nel romance scam il tempo è tutto. Le somme in criptovaluta e i fondi in stablecoin sono tracciabili e, in molti casi, congelabili; ma la finestra utile si misura in giorni, non in mesi. Chi si accorge di essere caduto nella trappola rende a sé stesso il servizio migliore quando smette di cercare una spiegazione rassicurante e si rivolge subito, insieme, alle autorità e a un legale.

PARTE PRIMA

Il fenomeno

Studio Legale Giammatteo



Che cos'è il romance scam

Una relazione affettiva simulata è lo strumento; l'obiettivo è il denaro. Comprendere la meccanica è il primo passo per riconoscerla e per collocarla correttamente sul piano giuridico.

UNA DEFINIZIONE OPERATIVA

Con l'espressione *romance scam*, o truffa romantica, si indica la condotta di chi costruisce una relazione sentimentale fittizia, in genere online, per indurre la persona corteggiata a trasferimenti di denaro o ad altre disposizioni patrimoniali. L'elemento distintivo non è il mezzo, ma la leva: al posto di un falso affare o di una falsa emergenza tecnica, l'artificio è un legame affettivo coltivato nel tempo. Il rapporto è il raggirio, e ogni richiesta economica ne è la conseguenza apparentemente naturale.

Sul piano giuridico, questa condotta trova la sua cornice principale nel delitto di truffa, che punisce chi, con artifici o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno. La relazione simulata è, appunto, l'artificio; la fiducia indotta è l'errore; il trasferimento di denaro è l'atto di disposizione dannoso.

PERCHÉ FUNZIONA

Il romance scam non fa leva sull'ingenuità, ma su bisogni universali: il desiderio di un legame, la solitudine, il lutto, una separazione. Per questo colpisce persone di ogni età e condizione, spesso lucide e prudenti in ogni altro ambito. L'autore lavora sul tempo: dedica settimane o mesi a costruire intimità e reciprocità prima di formulare la prima richiesta, quasi sempre modesta e giustificata da un'emergenza credibile. Quando arriva, il denaro non è più dato a uno sconosciuto, ma a una persona amata.

CHI C'È DIETRO

Dietro il singolo profilo opera di regola un'organizzazione, non un individuo isolato. Identità, fotografie e storie sono costruite e riutilizzate; i ruoli sono divisi; i flussi di denaro sono fatti transitare attraverso più conti e più Paesi per disperderne le tracce. Questa dimensione organizzata e transnazionale spiega perché la risposta efficace richie-

da, fin da subito, il coinvolgimento delle autorità e il ricorso agli strumenti di cooperazione, e perché la rapidità sia decisiva.



Come nasce e come si sviluppa

Il raggiro segue una progressione riconoscibile. Distinguerne le fasi aiuta a capire in quale punto ci si trova e quali condotte si stanno per compiere.

L'AGGANCIO

Il contatto avviene su app di incontri, social network, giochi online o messaggistica. Il profilo è curato e coerente: fotografie attraenti, una professione che giustifica assenze e distanza — militare all'estero, ingegnere su piattaforme offshore, medico in missione, imprenditore in viaggio. La distanza fisica non è un ostacolo, ma parte del copione: rende plausibile che non ci si possa mai incontrare.

LA COSTRUZIONE DEL LEGAME

Segue una fase di intensa comunicazione quotidiana. L'autore ascolta, ricorda, rassicura; anticipa progetti comuni; introduce presto il linguaggio dell'amore e dell'esclusività. È la fase in cui si crea la dipendenza affettiva che rende, poi, difficile dire di no e ancora più difficile riconoscere l'inganno anche di fronte all'evidenza.

LA PRIMA RICHIESTA E L'ESCALATION

La prima richiesta è quasi sempre contenuta e temporanea: una spesa medica, un problema doganale, un biglietto per il tanto atteso incontro. Una volta ottenuto il primo versamento, le richieste crescono per importo e frequenza, sostenute da nuove emergenze o da una prospettiva di guadagno condiviso. È qui che il romance scam si salda spesso con la truffa sugli investimenti: l'amore diventa il canale attraverso cui proporre un «affare» in criptovalute.

IL MANTENIMENTO E LA CHIUSURA

Finché la vittima paga, il rapporto prosegue e ogni dubbio viene disinnescato con spiegazioni sempre più elaborate. Quando le risorse si esauriscono o il sospetto diventa insostenibile, il contatto si interrompe. Non di rado, però, il percorso non finisce: i dati della vittima vengono ceduti e riutilizzati per un secondo tentativo, presentato come aiuto al recupero.



Le forme che assume oggi

La truffa affettiva si è evoluta e si combina con altre frodi. Riconoscerne le varianti serve a cogliere la pluralità delle condotte in gioco.

ROMANCE SCAM «PURO»

Nella forma classica, le richieste riguardano spese personali ed emergenze. Il denaro viene chiesto per necessità presentate come momentanee, con la promessa di restituzione e con la prospettiva dell'incontro che non arriva mai.

L'INNESTO SULL'INVESTIMENTO IN CRIPTOVALUTE

La variante oggi più diffusa e dannosa unisce la relazione affettiva alla proposta di investimento, spesso in criptovalute, su piattaforme che simulano rendimenti in crescita. Il partner virtuale «insegna» a investire e mostra guadagni fittizi, inducendo versamenti crescenti; quando la vittima chiede di prelevare, compaiono richieste di ulteriori pagamenti — commissioni, tasse, sblocchi — che rendono impossibile il rientro. È lo schema noto anche come *pig butchering*, l'«ingrasso» della vittima prima del prelievo definitivo.

LA DERIVA RICATTATORIA

In alcuni casi la relazione è finalizzata a ottenere immagini o video intimi, poi usati per estorcere denaro sotto la minaccia della diffusione. È la *sextortion*, che si colloca su un piano diverso e più grave rispetto alla semplice frode patrimoniale.

IL COINVOLGIMENTO OPERATIVO DELLA VITTIMA

Vi è infine la forma in cui la vittima non è soltanto chi paga, ma viene resa strumento della frode: le si chiede di ricevere somme di terzi e di ritrasferirle, di aprire conti o wallet, di prestare la propria identità. È la trasformazione della vittima in *money mule*, che apre problemi non solo di danno, ma di responsabilità personale, trattati più avanti.

PARTE SECONDA

Le condotte in cui la vittima può incappare

Studio Legale Giammatteo

L'invio di denaro

È la condotta più frequente e assume forme diverse, ognuna con implicazioni pratiche sulla tracciabilità e sul recupero.

BONIFICI E RICARICHE

Il bonifico bancario, anche internazionale, è il canale tipico. Presenta un vantaggio per la vittima: lascia una traccia documentale e, se segnalato con tempestività alla banca, può in alcuni casi essere bloccato o richiamato prima dell'accredito definitivo. Analoga tracciabilità offrono le ricariche di carte prepagate, spesso intestate a prestanome.

BUONI, GIFT CARD E CONTANTI

La richiesta di pagare con buoni regalo o carte regalo di circuiti commerciali, comunicandone i codici, è un segnale d'allarme in sé: nessuna esigenza legittima si soddisfa in quel modo. Questi strumenti, come l'invio di contanti tramite money transfer, sono i più difficili da tracciare e da recuperare, perché il valore è incassato in forma pressoché anonima.

PERCHÉ LA FORMA CONTA

La distinzione non è tecnica. Dalla forma del pagamento dipendono la possibilità di ricostruire il percorso del denaro, la rapidità con cui è possibile intervenire e la concreta prospettiva di recupero. Per questo, nel racconto al legale e nella denuncia, occorre indicare con precisione ogni operazione: data, importo, strumento, conto o wallet di destinazione.

NORMA DI RIFERIMENTO

La condotta di chi ottiene i versamenti integra, di regola, il delitto di **truffa** previsto dall'art. 640 del codice penale, procedibile a querela della persona offesa salvo i casi di procedibilità d'ufficio indicati dall'art. 649-bis c.p.

L'«investimento» su piattaforme fittizie

La vittima crede di investire e vede crescere un capitale che non esiste. La condotta si distingue dal semplice invio di denaro e merita un inquadramento proprio.

IL MECCANISMO

La vittima viene indirizzata verso un sito o un'app che imita una piattaforma di trading. Un cruscotto mostra depositi, rendimenti e grafici in crescita; talvolta è concesso un primo, piccolo prelievo, per consolidare la fiducia. Da quel momento si è indotti a versare somme crescenti. Al momento del prelievo dell'intero «capitale» compaiono ostacoli: commissioni di sblocco, imposte da anticipare, verifiche a pagamento. Nessuna di queste condizioni è reale: servono solo a estrarre altro denaro.

I SEGNALI

Ricorrono alcuni tratti costanti: una piattaforma non autorizzata a operare in Italia; l'assenza di una sede e di riferimenti verificabili; la pressione a decidere in fretta; l'assistenza di un «consulente» che segue passo passo; la richiesta di installare programmi di controllo remoto del dispositivo. La promessa di rendimenti elevati e sicuri è, di per sé, incompatibile con qualunque investimento serio.

NORME DI RIFERIMENTO

La condotta integra il delitto di **truffa** (art. 640 c.p.) e, quando l'inganno passa per l'alterazione del funzionamento di un sistema informatico o per l'intervento non autorizzato su dati e informazioni, il delitto di **frode informatica** previsto dall'art. 640-ter c.p.

Le criptovalute e i wallet

Il denaro in criptovaluta spaventa perché sembra sparire senza traccia. È vero il contrario: la tracciabilità è il principale alleato della vittima, a condizione di muoversi in fretta.

COME AVVIENE IL TRASFERIMENTO

Alla vittima viene chiesto di iscriversi a una piattaforma di scambio legittima, di acquistare criptovaluta con denaro proprio e di trasferirla verso un indirizzo esterno indicato dal truffatore, oppure verso la falsa piattaforma d'investimento. Spesso è la stessa vittima a compiere materialmente le operazioni, guidata passo passo. È frequente l'uso di *stablecoin*, criptovalute agganciate al valore di una valuta ufficiale.

TRACCIABILITÀ E CONGELAMENTO

Le operazioni in criptovaluta sono registrate su un registro pubblico e permanente. Ciò consente, con gli strumenti adeguati, di seguire il percorso dei fondi e di individuare gli indirizzi e gli intermediari verso cui confluiscano. Alcune *stablecoin* possono inoltre essere congelate dall'ente che le emette, su richiesta dell'autorità competente. Sono proprio queste due caratteristiche — tracciabilità e congelabilità — ad aprire margini concreti di recupero, che tuttavia si riducono con il passare dei giorni.

LA CONDOTTA DELLA VITTIMA

Sul piano giuridico, la vittima che acquista e trasferisce criptovaluta per effetto dell'inganno subisce una truffa, come chi effettua un bonifico. Diverso è il caso di chi movimentata criptovaluta di provenienza illecita per conto di terzi: quella condotta è trattata al capitolo sui rischi penali.

NORMA DI RIFERIMENTO

Restano applicabili gli artt. 640 e 640-ter c.p. La disciplina delle cripto-attività e degli obblighi antiriciclaggio degli operatori è richiamata al capitolo XIV.

La vittima come «money mule»

È la condotta più insidiosa, perché trasforma chi subisce in chi rischia. Va conosciuta con precisione, perché espone a una responsabilità penale propria.

COME ACCADE

Con la scusa di un aiuto, di un lavoro da casa o di una gestione «di coppia» delle finanze, alla vittima viene chiesto di ricevere sul proprio conto somme provenienti da terzi e di ritrasferirle altrove, trattenendo talvolta una piccola percentuale. Chi accetta diventa un anello della catena che ripulisce e disperde denaro di provenienza illecita: è il cosiddetto *money mule*, il «corriere» di denaro.

IL RISCHIO PROPRIO DELLA VITTIMA

Chi movimentava denaro altrui di provenienza delittuosa può rispondere, a seconda della consapevolezza e del ruolo, di ricettazione, di riciclaggio o di impiego di beni di provenienza illecita. La linea di confine è la conoscenza, anche solo eventuale, della provenienza illecita delle somme: chi accetta di operare «senza farsi troppe domande», di fronte a segnali evidenti, non è al riparo. Per questo è essenziale interrompere immediatamente ogni movimentazione e riferire tutto all'autorità: la posizione di chi si autodenuncia e collabora è ben diversa da quella di chi prosegue.

NORME DI RIFERIMENTO

Ricettazione (art. 648 c.p.); **riciclaggio** (art. 648-bis c.p.); **impiego di denaro, beni o utilità di provenienza illecita** (art. 648-ter c.p.); **autoriciclaggio** (art. 648-ter.1 c.p., introdotto dalla legge 15 dicembre 2014, n. 186). L'intera materia è stata rivista dal decreto legislativo 8 novembre 2021, n. 195, che ne ha ampliato l'ambito applicativo.

Le immagini intime e la sextortion

Quando la relazione è finalizzata a ottenere materiale intimo, il danno cambia natura: non è più solo economico, ma investe la dignità e la riservatezza della persona.

IL RICATTO

Ottenute immagini o video a contenuto sessuale, il truffatore minaccia di diffonderli — a familiari, colleghi, contatti — per estorcere denaro. La pressione psicologica è forte e immediata, e spinge la vittima a pagare nella speranza, quasi sempre delusa, di chiudere la vicenda. Cedere alimenta il ricatto: il pagamento è letto come conferma di vulnerabilità e apre a nuove richieste.

LA CONDOTTA CORRETTA

Occorre non pagare, conservare ogni elemento — profili, messaggi, richieste, identificativi di pagamento — e rivolgersi subito all'autorità. In caso di paventata o avvenuta diffusione di immagini a sfondo sessuale, esistono anche strumenti di intervento rapido attivabili presso l'Autorità Garante per la protezione dei dati personali, oltre alla tutela penale.

NORME DI RIFERIMENTO

Estorsione (art. 629 c.p.) per la minaccia finalizzata al pagamento; **diffusione illecita di immagini o video sessualmente espliciti** (art. 612-ter c.p., introdotto dalla legge 19 luglio 2019, n. 69) in caso di invio o diffusione del materiale senza consenso.

I dati, l'identità e gli accessi

Oltre al denaro, la vittima consegna spesso qualcosa di altrettanto prezioso: dati personali, documenti e credenziali. Le conseguenze possono durare oltre la fine del rapporto.

DOCUMENTI E IDENTITÀ

La richiesta di fotografie del documento d'identità, del codice fiscale o di un selfie con il documento — presentata come «verifica» per la piattaforma o per una spedizione — consente di aprire conti, sottoscrivere servizi o compiere ulteriori frodi a nome della vittima. Chi si spaccia per un'altra persona, o attribuisce a sé o ad altri un falso nome o stato, risponde di sostituzione di persona.

CREDENZIALI E ACCESSI REMOTI

L'invito a installare programmi di controllo remoto o a comunicare le credenziali di home banking o dei wallet consegna al truffatore il controllo diretto dei conti. L'accesso non autorizzato ai sistemi informatici e la loro manipolazione hanno una specifica rilevanza penale, autonoma rispetto alla truffa.

NORME DI RIFERIMENTO

Sostituzione di persona (art. 494 c.p.); **accesso abusivo a un sistema informatico o telematico** (art. 615-ter c.p.); **indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti** (art. 493-ter c.p.). La tutela dei dati personali è ripresa al capitolo XIII.

La seconda ondata: la truffa del recupero

Chi ha già subito un raggio è un bersaglio privilegiato per un secondo. La «truffa del recupero» promette di restituire il perduto e produce soltanto un'ulteriore perdita.

COME SI PRESENTA

A distanza di tempo, la vittima viene contattata da sedicenti società di consulenza, studi legali o «recovery agent» che dichiarano di poter recuperare le somme perdute, magari affermando di aver individuato i fondi o di collaborare con le autorità. La condizione è sempre la stessa: anticipare un pagamento — una percentuale, una cauzione, spese di procedura — o caricare un piccolo importo su un conto o su un exchange «per sbloccare» il trasferimento.

PERCHÉ DIFFIDARE

Nessun soggetto serio chiede denaro anticipato promettendo un recupero certo, né condiziona la restituzione al versamento di somme su piattaforme. Il recupero delle somme, quando è possibile, passa dalle autorità e dagli strumenti di legge, non da un pagamento preliminare a un intermediario che si è fatto avanti da solo. Spesso questi soggetti dispongono già dei dati della prima frode, segno che operano nello stesso ambiente.

NORMA DI RIFERIMENTO

Anche questa condotta integra il delitto di **truffa** (art. 640 c.p.), autonomo rispetto al primo raggio e da denunciare in quanto tale.

PARTE TERZA

Il quadro normativo

Studio Legale Giammatteo

I reati subiti dalla vittima

Le condotte descritte nella parte seconda trovano nel codice penale figure precise. Se ne richiama la sostanza, con l'indicazione dell'articolo, senza pretesa di completezza sulle circostanze.

LA TRUFFA

L'art. 640 c.p. punisce chi, con artifici o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno. È la figura centrale del romance scam. Il delitto è procedibile a querela della persona offesa; diventa procedibile d'ufficio nei casi indicati dall'art. 649-bis c.p., ad esempio in presenza di talune circostanze aggravanti.

LA FRODE INFORMATICA

L'art. 640-ter c.p. punisce chi, alterando il funzionamento di un sistema informatico o telematico o intervenendo senza diritto su dati, informazioni o programmi, procura a sé o ad altri un ingiusto profitto con altrui danno. Rileva quando l'inganno si realizza attraverso la manipolazione dei sistemi, tipica delle false piattaforme e degli accessi non autorizzati.

SOSTITUZIONE DI PERSONA E ACCESSO ABUSIVO

L'art. 494 c.p. (sostituzione di persona) colpisce chi induce altri in errore sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome o stato. L'art. 615-ter c.p. (accesso abusivo a un sistema informatico o telematico) tutela l'inviolabilità dei sistemi protetti, rilevante quando il truffatore ottiene o usa le credenziali della vittima.

ESTORSIONE E DIFFUSIONE DI IMMAGINI

Sul versante ricattatorio operano l'art. 629 c.p. (estorsione), per la minaccia diretta a ottenere il pagamento, e l'art. 612-ter c.p. (diffusione illecita di immagini o video sessualmente espliciti), per l'invio o la diffusione, senza consenso, di materiale a contenuto sessuale.

I rischi penali della vittima

È il capitolo che più spesso sorprende. Alcune condotte, se compiute con la consapevolezza della provenienza illecita del denaro, espongono la stessa vittima a responsabilità penale.

RICETTAZIONE, RICICLAGGIO E IMPIEGO

Chi riceve, occulta o trasferisce denaro sapendone la provenienza da delitto può rispondere di ricettazione (art. 648 c.p.). Chi compie operazioni volte a ostacolare l'identificazione della provenienza delittuosa di denaro o beni risponde di riciclaggio (art. 648-bis c.p.); chi li impiega in attività economiche o finanziarie risponde ai sensi dell'art. 648-ter c.p. Sono le figure entro cui ricade, tipicamente, il *money mule*.

L'AUTORICICLAGGIO

L'art. 648-ter.1 c.p. (autoriciclaggio), introdotto dalla legge 15 dicembre 2014, n. 186, punisce chi impiega, sostituisce o trasferisce in attività economiche, finanziarie o speculative il denaro o i beni provenienti da un delitto da lui stesso commesso, in modo da ostacolarne l'identificazione della provenienza.

IL CRITERIO DELLA CONSAPEVOLEZZA

Il discrimine è soggettivo: questi delitti richiedono la conoscenza della provenienza illecita, che può assumere anche la forma del dolo eventuale, ossia dell'accettazione consapevole del rischio. Chi opera trascurando segnali evidenti non può invocare, *sic et simpliciter*, la propria buona fede. Da qui l'indicazione pratica, ripetuta in questa guida: al primo dubbio, fermarsi e riferire tutto all'autorità.

NORME DI RIFERIMENTO

Artt. 648, 648-bis, 648-ter e 648-ter.1 c.p., come incisi dal decreto legislativo 8 novembre 2021, n. 195; art. 493-ter c.p. per l'indebito utilizzo di strumenti di pagamento diversi dai contanti.

La tutela dei dati personali

La sottrazione e l'uso illecito di dati, documenti e immagini hanno una tutela propria, che affianca quella penale e offre strumenti rapidi.

IL QUADRO

Il trattamento dei dati personali è regolato dal Regolamento (UE) 2016/679 (GDPR) e, in Italia, dal Codice in materia di protezione dei dati personali (decreto legislativo 30 giugno 2003, n. 196, come modificato dal decreto legislativo 10 agosto 2018, n. 101). L'uso dei dati della vittima per aprire conti, sottoscrivere servizi o diffondere immagini è un trattamento illecito.

GLI STRUMENTI

Sul piano penale, il trattamento illecito di dati è previsto dall'art. 167 del Codice privacy. Sul piano amministrativo, la vittima può rivolgersi all'Autorità Garante per la protezione dei dati personali, anche con segnalazione o reclamo; in materia di immagini a sfondo sessuale sono previste procedure di intervento tempestivo. Restano fermi i diritti riconosciuti dal GDPR, tra cui la cancellazione dei dati e l'opposizione al trattamento.

NORME DI RIFERIMENTO

Reg. (UE) 2016/679; d.lgs. 30 giugno 2003, n. 196, e in particolare l'art. 167 (trattamento illecito di dati).

Cripto-attività e antiriciclaggio

La dimensione in criptovaluta ha una cornice regolatoria che è utile conoscere, perché su di essa poggiano gli obblighi degli operatori e, indirettamente, le possibilità di intervento.

GLI OBBLIGHI ANTIRICICLAGGIO

Gli operatori che prestano servizi relativi all'uso di valute virtuali e di portafogli digitali sono soggetti alla disciplina antiriciclaggio dettata dal decreto legislativo 21 novembre 2007, n. 231, che impone adeguata verifica della clientela, conservazione dei dati e segnalazione delle operazioni sospette alla Unità di Informazione Finanziaria. L'inclusione dei prestatori di servizi in valuta virtuale tra i soggetti obbligati è avvenuta con il decreto legislativo 4 ottobre 2019, n. 125, di recepimento della cosiddetta quinta direttiva antiriciclaggio.

REGISTRAZIONE DEGLI OPERATORI E MICA

In Italia, gli operatori in valute virtuali sono tenuti all'iscrizione presso l'Organismo Agenti e Mediatori (OAM), secondo le modalità fissate con decreto del Ministero dell'Economia e delle Finanze del 13 gennaio 2022. Sul piano europeo, il Regolamento (UE) 2023/1114 (MiCA) ha introdotto un quadro organico per le cripto-attività e per i relativi prestatori di servizi. Questi obblighi, gravando su exchange e intermediari, rendono più agevole, per l'autorità, l'individuazione dei soggetti e delle operazioni.

NORME DI RIFERIMENTO

D.lgs. 21 novembre 2007, n. 231; d.lgs. 4 ottobre 2019, n. 125; D.M. MEF 13 gennaio 2022; Reg. (UE) 2023/1114 (MiCA).

I profili civili

Accanto alla via penale, il diritto civile offre strumenti per ottenere il risarcimento del danno e la restituzione di quanto versato, verso i soggetti che sia possibile individuare.

IL RISARCIMENTO DEL DANNO

Chi ha cagionato il danno con il proprio fatto illecito è tenuto a risarcirlo, ai sensi dell'art. 2043 del codice civile; il danno non patrimoniale è risarcibile nei casi previsti dalla legge, secondo l'art. 2059 c.c. La pretesa può essere fatta valere anche nel processo penale, mediante costituzione di parte civile.

LA RESTITUZIONE DELL'INDEBITO

Chi ha eseguito un pagamento non dovuto ha diritto di ripetere ciò che ha pagato, secondo l'art. 2033 c.c. Lo strumento assume rilievo quando le somme siano individuabili presso un soggetto tenuto alla restituzione.

IL LIMITE PRATICO

Il limite di questi rimedi è l'identificabilità e la solvibilità della controparte: verso un autore ignoto e all'estero, la via civile è spesso poco efficace. Per questo, nel romance scam, l'azione civile è di regola complementare a quella penale e agli strumenti di sequestro e confisca, non alternativa.

NORME DI RIFERIMENTO

Artt. 2043, 2059 e 2033 del codice civile; costituzione di parte civile ai sensi degli artt. 74 e seguenti del codice di procedura penale.

PARTE QUARTA

Cosa fare

Studio Legale Giammatteo

Denuncia e querela

È il primo atto formale e va compiuto senza indugio. Alcune distinzioni ne governano tempi e modi.

DENUNCIA E QUERELA

La denuncia (art. 333 c.p.p.) è la notizia di un reato portata all'autorità; la querela (artt. 336 e seguenti c.p.p.) è la manifestazione di volontà, della persona offesa, che il fatto sia perseguito, necessaria per i reati procedibili a querela. La truffa, di regola procedibile a querela, richiede dunque questa manifestazione di volontà entro il termine di legge.

IL TERMINE

Il diritto di querela si esercita, salvo diversa previsione, entro tre mesi dal giorno in cui si è avuta notizia del fatto che costituisce reato, secondo l'art. 124 c.p. Il termine è perentorio: la sua conoscenza è essenziale, perché nel romance scam la consapevolezza dell'inganno arriva spesso a distanza dai primi versamenti.

COSA PORTARE

È utile raccogliere e ordinare, prima possibile, ogni elemento: profili e conversazioni, contabili dei bonifici e delle ricariche, indirizzi dei wallet, ricevute delle piattaforme, nominativi e recapiti utilizzati dal truffatore. Un fascicolo ordinato accelera le indagini e sostiene le eventuali richieste di blocco e sequestro.

Congelamento, sequestro e confisca

Sono gli strumenti che possono bloccare e, poi, sottrarre definitivamente il denaro all'autore. La loro efficacia dipende dalla rapidità.

IL SEQUESTRO

Nel processo penale, il sequestro preventivo (art. 321 c.p.p.) consente di bloccare beni e disponibilità collegati al reato, così da impedirne la dispersione. Verso somme e criptoattività individuate, è lo strumento che «ferma» i valori in vista della confisca.

LA CONFISCA, ANCHE PER EQUIVALENTE

La confisca (art. 240 c.p.) sottrae definitivamente il profitto del reato. Per la truffa e la frode informatica, l'art. 640-quater c.p. richiama la disciplina della confisca per equivalente prevista dall'art. 322-ter c.p.: quando il profitto diretto non è aggredibile, la sottrazione può colpire beni di valore corrispondente.

LA DIMENSIONE TRANSFRONTALIERA

Poiché i fondi transitano quasi sempre all'estero, assume rilievo il Regolamento (UE) 2018/1805, che disciplina il riconoscimento reciproco, tra gli Stati membri, dei provvedimenti di congelamento e di confisca, semplificandone l'esecuzione oltre confine. È lo strumento che rende possibile aggredire valori collocati in un altro Paese dell'Unione.

NORME DI RIFERIMENTO

Art. 321 c.p.p.; artt. 240, 322-ter e 640-quater c.p.; Reg. (UE) 2018/1805.

Il recupero delle somme

Recuperare è possibile, ma non è né automatico né immediato. Conta agire per canali legittimi e nel più breve tempo possibile.

LA SEGNALAZIONE AGLI INTERMEDIARI

La prima mossa, in parallelo alla denuncia, è la segnalazione tempestiva alla propria banca o all'emittente della carta e, se identificabile, alla piattaforma di scambio verso cui sono confluiti i fondi. Per i bonifici non ancora accreditati esistono margini di richiamo; per le cripto-attività, la segnalazione all'exchange e il congelamento delle stablecoin, se disposto dall'autorità, possono bloccare i valori.

LA PARTE CIVILE E LE ALTRE VIE

Nel processo penale, la vittima può costituirsi parte civile per ottenere il risarcimento; in caso di sequestro e confisca, potrà far valere le proprie ragioni sui valori recuperati. Verso soggetti individuati e solvibili resta esperibile l'azione civile autonoma per il risarcimento e la restituzione.

LA DIFFIDENZA NECESSARIA

Nessun recupero passa da un pagamento anticipato a un intermediario che si è proposto spontaneamente promettendo la restituzione: è, semmai, il segno di una seconda truffa. Il recupero legittimo passa dalle autorità, dagli intermediari regolati e dagli strumenti di legge.

Prevenzione e segnali d'allarme

La difesa migliore resta il riconoscimento precoce. Alcuni segnali ricorrono e, presi insieme, valgono più di ogni rassicurazione.

I SEGNALI DEL RAPPORTO

Una persona conosciuta solo online che, nonostante l'intensità del legame, non si mostra mai in videochiamata e non può mai incontrarsi; una storia che giustifica sempre la distanza; una progressione rapida verso l'intimità e l'esclusività. Sono i tratti costitutivi del copione.

I SEGNALI ECONOMICI

La prima richiesta di denaro, per quanto piccola e motivata; la proposta di un investimento sicuro e redditizio; la pressione a decidere in fretta; la richiesta di pagare con buoni regalo, ricariche o criptovaluta; l'invito a installare programmi di controllo remoto o a comunicare credenziali e documenti. Ognuno di questi elementi, da solo, giustifica una verifica; la loro somma è quasi sempre una truffa.

LA REGOLA PRATICA

Non inviare denaro a chi non si è mai incontrato di persona; non condividere documenti, credenziali o immagini intime; non pagare per «sbloccare» un prelievo. E, soprattutto, non affrontare la vicenda da soli: al primo dubbio, conservare tutto e rivolgersi insieme alle autorità e a un legale. Nel romance scam, come si è detto, la differenza la fa il tempo.

L'autore

L'Avv. Gianluca Giammatteo, del Foro di Isernia, è Patrocinante in Cassazione. Lo Studio Legale Giammatteo, con sede in Venafro (IS), assiste privati e imprese in materia civile e penale, con particolare attenzione alle frodi online, alle truffe in criptovalute e alla tutela della reputazione e dei dati personali.

Lo Studio segue le vittime di truffe affettive e di frodi sugli investimenti in ogni fase: dalla denuncia e dalla querela alle richieste di blocco, sequestro e confisca, fino alla costituzione di parte civile e alle azioni per il recupero delle somme, avvalendosi anche degli strumenti di cooperazione europea.

www.giammatteo.it – Via Nicandro Iosso n. 6, 86079 Venafro (IS)

Nota e fonti normative

Il presente testo ha finalità informativa e formativa e non contiene riferimenti giurisprudenziali. Le disposizioni richiamate sono aggiornate al mese di luglio 2026 e vanno verificate, nella loro versione vigente, prima di ogni impiego in atti giudiziari. L'inquadramento delle singole condotte dipende dai fatti concreti e richiede l'esame del caso.

CODICE PENALE

Art. 494 (sostituzione di persona); art. 615-ter (accesso abusivo a un sistema informatico o telematico); art. 493-ter (indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti); art. 629 (estorsione); art. 612-ter (diffusione illecita di immagini o video sessualmente espliciti); art. 640 (truffa); art. 640-ter (frode informatica); art. 640-quater e art. 322-ter (confisca per equivalente); art. 240 (confisca); art. 648 (ricettazione); art. 648-bis (riciclaggio); art. 648-ter (impiego di denaro, beni o utilità di provenienza illecita); art. 648-ter.1 (autoriciclaggio); art. 649-bis (casi di procedibilità d'ufficio); art. 124 (termine per la querela).

CODICE CIVILE E DI PROCEDURA PENALE

Codice civile: artt. 2043, 2059 e 2033. Codice di procedura penale: art. 333 (denuncia); artt. 336 e seguenti (querela); artt. 74 e seguenti (parte civile); art. 321 (sequestro preventivo).

LEGGI, DECRETI E FONTI EUROPEE

Legge 15 dicembre 2014, n. 186 (autoriciclaggio); legge 19 luglio 2019, n. 69 (introduzione dell'art. 612-ter c.p.); decreto legislativo 8 novembre 2021, n. 195 (riforma dei reati in materia di riciclaggio); decreto legislativo 21 novembre 2007, n. 231 (antiriciclaggio); decreto legislativo 4 ottobre 2019, n. 125; decreto del Ministero dell'Economia e delle Finanze del 13 gennaio 2022 (registrazione degli operatori in valute virtuali presso l'OAM); decreto legislativo 30 giugno 2003, n. 196, e decreto legislativo 10 agosto 2018, n. 101 (Codice privacy); Regolamento (UE) 2016/679 (GDPR); Regolamento (UE) 2018/1805 (riconoscimento reciproco dei provvedimenti di congelamento e di confisca); Regolamento (UE) 2023/1114 (MiCA).