Metodo Giuridico
Ius et Ratio
ISSN 3103-7305

Frode informatica e identità digitale estesa all'home banking

La Cassazione (sent. n. 25792/2026) chiarisce i confini dell'aggravante ex art. 640-ter c.p., la validità della contestazione in fatto e la presunzione sul percettore del bonifico

Redazione di Metodo Giuridico Diritto Penale 27 Agosto 2026 Lettura 12 min

Stato della questione e quadro aggiornato al 27 Agosto 2026: Con la sentenza n. 25792 depositata il 9 luglio 2026, la Seconda Sezione Penale della Cassazione stabilisce che l'aggravante del furto di identità digitale ex art. 640-ter comma 3 c.p. include l'uso di credenziali home banking private, può essere contestata in fatto e pone a carico del correntista beneficiario l'onere di allegare circostanze idonee a superare la massima di esperienza di concorso nell'illecito.

Abstract (Italiano)

La Corte di Cassazione, con la sentenza n. 25792 del 9 luglio 2026, affronta i nodi centrali del binomio tra **frode informatica e identità digitale**, delineando l'ambito applicativo dell'aggravante ad effetto speciale di cui all'art. 640-ter, terzo comma, c.p. La Suprema Corte chiarisce che la **nozione penalistica di identità digitale** non è limitata ai soli **sistemi pubblici di autenticazione** validati dalla Pubblica Amministrazione, ma ricomprende qualsiasi insieme di credenziali e **codici dispositivi** utilizzati per accedere a piattaforme telematiche private di **home banking**. Viene inoltre sancita la piena legittimità della **contestazione in fatto** dell'aggravante quando l'imputazione ne descriva compiutamente i tratti materiali, senza lesione del **principio di correlazione** ex art. 521 c.p.p. Sul versante probatorio, l'accredito delle somme carpite sul **conto corrente** dell'imputato costituisce **massima di esperienza** idonea a fondare la responsabilità, gravando su quest'ultimo l'**onere di allegazione** specifica in virtù del **principio di vicinanza della prova**.

Abstract (English)

In Judgment No. 25792 of July 9, 2026, the Italian Court of Cassation clarifies the legal boundaries governing computer fraud and digital identity theft under Art. 640-ter, paragraph 3, of the Italian Criminal Code. The Court rules that the criminal concept of digital identity is not restricted to public authentication systems validated by public authorities, but extends to private online banking access

Metodo Giuridico
Ius et Ratio
ISSN 3103-7305

credentials and security tokens. The judgment confirms that the aggravating circumstance may be lawfully charged de facto, provided that the indictment precisely details the material conduct. Furthermore, on the evidentiary plane, the receipt of fraudulent funds into a bank account constitutes a presumption of culpability under common experience rules, placing on the account holder the burden of substantiating specific factual alternatives under the principle of proximity of evidence.

Punti Chiave dell'Analisi

- **Nozione Estesa di Identità Digitale:** Ai fini dell'art. 640-ter, comma 3, c.p., l'identità digitale include i codici di accesso e le credenziali di home banking gestite da istituti privati.
- **Irrilevanza della Fonte di Acquisizione:** L'aggravante sussiste anche qualora le credenziali siano state carpite da terzi rimasti ignoti e successivamente utilizzate dall'imputato.
- **Piena Validità della Contestazione in Fatto:** L'aggravante è validamente applicata se il capo d'imputazione descrive l'accesso abusivo in sostituzione del titolare, senza violazione dell'art. 521 c.p.p.
- **Massima di Esperienza sull'Accredito:** Il percettore del bonifico fraudolento è presunto autore o concorrente nel reato in base a criteri di normalità causale.
- **Onere di Allegazione e Vicinanza della Prova:** Spetta all'imputato allegare elementi concreti di estraneità o di intestazione fittizia del conto per superare la presunzione d'accusa ex art. 192 c.p.p.

Principio di Diritto (Cass. pen., Sez. II, sent. 9 luglio 2026, n. 25792)

In tema di frode informatica, la circostanza aggravante dell'indebito utilizzo dell'identità digitale di cui all'art. 640-ter, terzo comma, cod. pen. non presuppone una procedura di validazione adottata dalla Pubblica amministrazione, trovando applicazione anche nel caso di utilizzo di credenziali di accesso e codici dispositivi a sistemi informatici di home banking gestiti da enti privati. È ammissibile la contestazione in fatto di detta aggravante qualora l'imputazione individui nella loro materialità i comportamenti costitutivi, rendendo autoevidente la circostanza e garantendo il diritto di difesa ex art. 521 cod. proc. pen. Inoltre, costituisce massima di esperienza il fatto che colui il quale percepisce il profitto dell'illecito ricevendone l'accredito sul proprio conto corrente sia anche colui che ha posto in essere la condotta o vi abbia concorso, gravando sull'imputato l'onere di

> *allegare concreti e oggettivi elementi fattuali idonei a collocarlo al di fuori della catena causale tipica in applicazione del principio della vicinanza della prova.*

01. Introduzione: la pronuncia Cass. Pen. n. 25792/2026

Con la **sentenza 9 luglio 2026, n. 25792**, la Seconda Sezione Penale della Corte di Cassazione interviene con un pronunciamento di **primario rilievo sistematico** sul nesso intercorrente tra **frode informatica e identità digitale**, sciogliendo delicati quesiti inerenti all'**aggravante ad effetto speciale** di cui all'art. 640-ter, terzo comma, c.p. e al governo dell'**onere probatorio** nel processo penale[1]. La Suprema Corte consolida una lettura rigorosa delle condotte di **cyber-fraud bancaria**, offrendo importanti **coordinate interpretative** sia sul piano sostanziale sia su quello processuale.

La pronuncia si articola su una **duplice direttrice nomofilattica**: da un lato, l'affermazione dell'**autonomia concettuale dell'identità digitale** penalmente protetta, la cui sussistenza non dipende dai rigidi schemi pubblicistici dei **sistemi di validazione statale** (quali SPID o CIE), ma abbraccia pienamente le **credenziali di accesso** a circuiti privati di **home banking**; dall'altro lato, la validazione della **contestazione in fatto delle circostanze aggravanti** e la razionalizzazione della **massima di esperienza** che ancora la **responsabilità concorsuale** all'effettiva ricezione del **profitto illecito** sul conto corrente.

1.1 — Il quadro dei reati informatici tra accesso abusivo e frode patrimoniale

Nel sistema penale dell'era digitale, la **linea di demarcazione** tra l'accesso abusivo a un sistema informatico o telematico ex art. 615-ter c.p. e la fattispecie di frode informatica di cui all'art. 640-ter c.p. risiede nell'**oggettività giuridica** e nella **dinamica lesiva** della condotta. Mentre l'art. 615-ter c.p. tutela il **domicilio informatico** quale spazio virtuale riservato contro intrusioni non autorizzate o **sviamenti funzionali** del potere di accesso, come chiarito dalle Sezioni Unite nella nota **sentenza Savarese**[2] e ribadito in relazione alle **finalità d'ufficio**[3], l'art. 640-ter c.p. presidia il **patrimonio individuale** contro le manipolazioni telematiche che alterano i processi di **elaborazione e trasferimento** dei dati economici[4].

La frode informatica si differenzia dalla **truffa comune** di cui all'art. 640 c.p. per il fatto che l'**attività ingannatoria** non investe la persona fisica della vittima – determinandone un **vizio del consenso** attraverso artifici e raggiri –, bensì agisce direttamente sulla macchina e sui **flussi informativi automatizzati**. La condotta decettiva si consuma nel momento in cui l'agente consegue l'**ingiusto profitto patrimoniale** mediante l'**alterazione del sistema** o l'intervento non autorizzato su dati e programmi, integrando una fattispecie complessa frequentemente associata a **delitti contro il patrimonio** o tentativi estorsivi[5].

In questo scenario, l'introduzione dell'aggravante del **furto o indebito utilizzo dell'identità digitale** nel 2013 ha inteso apprestare una **tutela rafforzata** contro le fenomenologie di **impersonificazione telematica**, dove la sottrazione o l'uso indebito di **credenziali univoche** consente all'aggressore di operare all'interno dei **conti correnti bancari** simulando la titolarità legittima del **rapporto contrattuale**.

1.2 — La vicenda processuale: la frode di home banking e l'imputazione a carico del correntista

Il procedimento penale sfociato nella decisione della Suprema Corte trae origine da una complessa operazione fraudolenta ai danni di una correntista di un primario istituto di credito. Soggetti rimasti non identificati avevano carpite le credenziali di accesso telematico al conto online della vittima, inserendosi abusivamente nel sistema e disponendo un **bonifico bancario non autorizzato** per un importo di **19.901 euro** a favore del conto corrente intestato all'imputato.

Il Giudice dell'udienza preliminare del **Tribunale di Genova** condannava l'imputato per concorso nei reati di cui agli artt. 615-ter e 640-ter c.p., applicando l'aggravante dell'**indebito utilizzo dell'identità digitale** ex art. 640-ter, comma 3, c.p. La **Corte d'Appello di Genova** confermava integralmente la statuizione di responsabilità, rigettando le censure difensive relative alla **mancata contestazione formale** dell'aggravante e alla pretesa insufficienza del mero accredito bancario quale prova del **concorso colposo o doloso** nel reato.

Proposto ricorso per cassazione, la difesa lamentava la **violazione del principio di correlazione tra imputazione e sentenza** ex artt. 441 e 522 c.p.p. per l'applicazione dell'aggravante non richiamata espressamente nel capo d'accusa, nonché la violazione dei canoni della **prova indiziaria** ex art. 192 c.p.p., sostenendo che la sola **titolarità del conto ricevente** non potesse fondare un giudizio di colpevolezza oltre ogni ragionevole dubbio.

Metodo Giuridico
Ius et Ratio
ISSN 3103-7305

02. La nozione penalistica di identità digitale nell'art. 640-ter c.p.

Il fulcro dogmatico della sentenza n. 25792/2026 consiste nella precisa **perimetrazione concettuale** della **nozione di identità digitale** nell'ambito della fattispecie incriminatrice dell'art. 640-ter, comma 3, c.p. Superando i tentativi di circoscrivere l'aggravante alle sole **identità certificate** nell'ambito del Codice dell'Amministrazione Digitale, la Suprema Corte riafferma che il concetto penalmente rilevante possiede una **matrice funzionale e oggettiva**, volta a tutelare l'**univocità della rappresentazione telematica** del soggetto all'interno di qualsiasi piattaforma informatica complessa, in perfetta consonanza con i principi generali che governano le **sanzioni e le confische ablative** nei reati contro il patrimonio[D1].

Come già chiarito dalla giurisprudenza di legittimità nei precedenti specifici in tema di **servizi telematici**[6], l'identità digitale deve essere intesa come l'insieme delle **informazioni e delle risorse** concesse da un sistema informatico ad un determinato utilizzatore mediante una **procedura di identificazione**, consistente nella validazione di dati attribuiti in modo esclusivo che ne consentono l'individuazione e la **legittimazione operativa**.

> « L'identità digitale penalmente rilevante include le credenziali di home banking private: l'impiego abusivo dei codici integra l'aggravante anche senza certificazione pubblica statale. »

Ne discende che l'accesso fraudolento al conto bancario online mediante l'utilizzo dei **codici cliente**, delle **password di sicurezza** o dei **token dispositivi** della persona offesa integra a pieno titolo la fattispecie aggravata: l'agente non si limita a violare una barriera tecnica, ma **surroga la volontà negoziale** della vittima, presentandosi verso l'ente bancario quale **titolare legittimo** della disponibilità finanziaria. La ratio dell'aggravamento sanzionatorio si fonda precisamente sul **maggiore disvalore sociale** dell'azione, la quale sfrutta la vulnerabilità dell'ambiente digitale per aggirare i **presidi fiduciari** del sistema creditizio.

L'approdo ermeneutico della Suprema Corte risponde alle esigenze di **effettività della tutela penale**: ancorare la nozione di identità digitale a formali **procedure pubbliche** avrebbe svuotato di significato l'aggravante nei confronti della quasi totalità delle frodi informatiche commesse ai danni di **privati e consumatori** nel settore dei **pagamenti digitali**.

03. La contestazione in fatto dell'aggravante e le garanzie difensive

Il secondo pilastro su cui riposa la decisione in commento riguarda i **requisiti formali di validità** dell'atto d'accusa, con particolare riferimento all'ammissibilità della **contestazione in fatto delle circostanze aggravanti** e alla salvaguardia delle **prerogative difensive** dell'imputato nel quadro di **frode informatica e identità digitale**, in aderenza ai canoni costituzionali del **giusto processo** e di **tassatività dell'azione punitiva**[D2].

3.1 — I requisiti di specificità dell'imputazione ex art. 521 c.p.p.

Il principio di **necessaria correlazione** tra l'accusa formulata e la sentenza emessa, sancito dall'art. 521 c.p.p. e presidiato dalla **nullità insanabile** di cui all'art. 522 c.p.p., mira a garantire che l'imputato sia posto nelle condizioni di esercitare un **diritto di difesa pieno ed effettivo** sul fatto storico ascrittogli. La giurisprudenza di legittimità ha progressivamente chiarito che tale garanzia non impone la rigida **indicazione numerica** dell'articolo di legge o del comma violato, bensì la puntuale e inequivoca **descrizione materiale degli elementi costitutivi** della fattispecie circostanziale[7], assicurando la perfetta tenuta del **contraddittorio processuale**[8].

Nel caso esaminato, il capo di imputazione descriveva espressamente la **condotta degli agenti** che, dopo essersi procurati in modo non autorizzato gli **estremi identificativi** e il codice di accesso per operare sul conto corrente online della banca, erano intervenuti senza diritto sul sistema telematico dell'istituto operando direttamente in **sostituzione della titolare**. Tale formulazione è stata considerata pienamente sufficiente a rendere **autoevidente la condotta** di sostituzione telematica, escludendo qualsivoglia compressione del diritto di difesa o **mutamento a sorpresa** del quadro accusatorio.

3.2 — L'autoevidenza del fatto materiale e l'assenza di profili valutativi

Perché la contestazione in fatto sia legittima, la circostanza deve emergere dal testo dell'imputazione in termini di **pura evidenza storica**, senza presupporre apprezzamenti o **qualificazioni giuridiche implicite** non esplicitate dal pubblico ministero[9]. La distinzione tra **circostanze valutative** (quali l'ingente danno patrimoniale o la particolare gravità) e **circostanze fattuali-descrittive** (quali i mezzi adoperati o l'identità digitale violata) è dirimente[10].

Mentre le prime richiedono una manifestazione espressa affinché la difesa possa interloquire sui **parametri estimativi**, le seconde si risolvono nell'**accertamento empirico** dell'azione descritta nella rubrica: una volta provato l'utilizzo abusivo delle **credenziali personali altrui**, l'aggravante di cui all'art. 640-ter, comma 3, c.p. opera quale necessaria e automatica **qualificazione giuridica** del fatto contestato.

3.3 — L'utilizzo di credenziali carpite da terzi e la cooperazione nell'illecito

Un ulteriore aspetto di notevole rilevanza attiene alla **dissociazione temporale e soggettiva** tra la fase di sottrazione dei dati di accesso e la fase di disposizione patrimoniale. La Cassazione ribadisce che l'aggravante dell'indebito utilizzo dell'identità digitale sussiste anche qualora le credenziali siano state originariamente **acquisite da soggetti terzi** rimasti ignoti (ad esempio mediante **campagne massive di phishing** o malware) e successivamente messe a disposizione del concorrente[11].

Ciò che conta ai fini del perfezionamento del reato e della relativa aggravante non è la **modalità genetica** con cui il codice è stato reperito, bensì l'**impiego consapevole e finalizzato** dello stesso per disporre operazioni patrimoniali illegittime, integrandosi il pieno **concorso criminoso** in capo a tutti i soggetti che partecipano alla **catena esecutiva** del raggiro telematico.

Profilo di Analisi	Tesi Difensiva Reietta	Principio Affermato dalla Cassazione
Ambito Identità Digitale	Riferita esclusivamente a sistemi pubblici di autenticazione validati dalla P.A. (SPID, CIE)	Estesa a qualsiasi credenziale e codice di accesso univoco a piattaforme private di home banking
Modalità di Contestazione	Necessità di espressa indicazione dell'art. 640-ter comma 3 c.p. a pena di nullità ex art. 522 c.p.p.	Piena validità della contestazione in fatto se la condotta materiale è descritta chiaramente
Origine delle Credenziali	Inapplicabilità dell'aggravante se i codici sono stati carpite da terzi e non dall'imputato	Sussistenza dell'aggravante per il consapevole utilizzo dispositivo delle credenziali illecite
Prova del Concorso	Insufficienza del solo accredito sul conto corrente per assenza di pluralità indiziaria	Massima di esperienza di autoria/concorso con onere di allegazione a carico dell'imputato

04. Regime probatorio, massime di esperienza e vicinanza della prova

Sul piano processuale, la sentenza n. 25792/2026 affronta con lucidità dogmatica uno dei nodi più complessi nella repressione delle frodi informatiche: l'**efficacia dimostrativa** della titolarità del **rapporto bancario di destinazione** delle somme nell'ambito di **frode informatica e identità digitale**.

4.1 — La presunzione di responsabilità legata all'accredito sul conto corrente

La difesa del ricorrente deduceva che l'accredito sul conto corrente rappresentasse un **indizio isolato**, inidoneo a soddisfare i rigidi requisiti di gravità, precisione e concordanza prescritti dall'art. 192, comma 2, c.p.p. La Corte di Cassazione respinge tale impostazione, riaffermando che nei reati contro il patrimonio il conseguimento del profitto non costituisce un **accadimento estrinseco o neutrale**, bensì l'**evento teleologico e funzionale** dell'intera condotta illecita[12].

In base a una consolidata **massima di esperienza** fondata sull'id quod plerumque accidit, colui che riceve sul proprio conto personale le somme fraudolentemente sottratte alla vittima deve presumersi l'**autore materiale dell'artifizio** ovvero il **concorrente consapevole** nell'operazione decettiva, apparendo irragionevole ipotizzare che un'organizzazione criminale trasferisca il provento di un reato a beneficio di un soggetto totalmente ignaro ed estraneo alla **dinamica criminosa**[13].

4.2 — L'onere di allegazione dell'imputato tra presunzione di innocenza e vicinanza probatoria

La Suprema Corte affronta con rigore il delicato tema della compatibilità tra tale massima di esperienza e la **presunzione di non colpevolezza** sancita dall'art. 27, secondo comma, Cost. Il Collegio esclude fermamente che si sia in presenza di un'**illegittima inversione** dell'onere della prova: una volta che la pubblica accusa abbia provato la **titolarità esclusiva** del conto e l'accreditamento della somma provento di reato, scatta in capo all'imputato un **onere di allegazione contraria** fondato sul principio generale di **vicinanza della prova**[14].

Per superare la **presunzione di autoria** o correità, la difesa non può limitarsi a formulare **smentite apodittiche** o congetture generiche, ma è tenuta a fornire **elementi fattuali concreti** e oggettivamente verificabili idonei a collocare l'imputato al di fuori della serie causale (ad esempio la prova di un furto d'identità a sua volta subito, l'avvenuto **disconoscimento del conto** o la dimostrazione di un utilizzo abusivo operato da terzi delegati).

05. Profili sistematici e ricadute operative per la difesa penale

Le conclusioni raggiunte dalla Seconda Sezione Penale nella sentenza n. 25792/2026 tracciano **linee guida fondamentali** per i difensori penali impegnati nei procedimenti per **cyber-crime e reati patrimoniali telematici** in tema di **frode informatica e identità digitale**.

5.1 — Il fenomeno dei money mule e la prova del dolo concorsuale

La prassi giudiziaria dimostra come in moltissimi casi i titolari dei conti correnti di destinazione siano soggetti terzi (spesso definiti **money mule** o **prestanome digitali**) reclutati con promesse di guadagni facili o mediante **false offerte di lavoro online**. L'arresto di legittimità in esame ribadisce che la messa a disposizione del proprio conto per il transito di fondi illeciti è sufficiente a integrare il **dolo eventuale di concorso** nel reato di frode informatica, qualora l'imputato abbia accettato consapevolmente il rischio dell'**origine delittuosa** delle somme.

La tesi dell'**inconsapevolezza totale** regge soltanto qualora emergano **riscontri documentali** attestanti l'inganno subito dal titolare del conto ovvero la **pronta segnalazione** agli organi di polizia e all'istituto bancario non appena pervenuta la notizia del **bonifico anomalo**.

5.2 — Protocolli difensivi e verifica della catena causale alternativa

Alla luce dei principi espressi dalla Suprema Corte, l'impostazione della **strategia difensiva** nei procedimenti per frode informatica aggravata deve articolarsi secondo **quattro direttrici metodologiche prioritarie**:

In primo luogo, in sede di **udienza preliminare** o di giudizio di primo grado, è necessario condurre un **vaglio rigoroso del capo d'imputazione**: qualora la contestazione dell'aggravante sia avvenuta in fatto ma l'atto d'accusa manchi della **precisa indicazione dei mezzi materiali** di impersonificazione o presenti elementi ambigui, la difesa dovrà eccepire tempestivamente la violazione dell'art. 521 c.p.p.

In secondo luogo, sul piano dell'**istruttoria dibattimentale**, la difesa del correntista deve procedere all'**immediata acquisizione dei file di log** bancari e dei **tabulati telematici**, al fine di verificare se le **sessioni di accesso** al conto siano state generate da **indirizzi IP**, dispositivi hardware o **localizzazioni geografiche** totalmente incompatibili con l'imputato.

In terzo luogo, occorre documentare analiticamente la **destinazione finale delle somme**: dimostrare che il denaro accreditato è stato **immediatamente prelevato o stornato** verso conti esteri tramite credenziali carpite all'imputato stesso è elemento fondamentale per vincere la **massima di esperienza** di profitto personale.

Infine, la valorizzazione di **denunce di smarrimento documenti**, querele preventive o **contestazioni verso l'istituto di credito** consentirà di soddisfare pienamente l'**onere di allegazione** richiesto dalla

Suprema Corte, riconducendo il giudizio di responsabilità entro i confini invalicabili del **ragionevole dubbio** presidiato dall'art. 111 Cost.

Fonti Utilizzate

Normativa di riferimento

Art. 640-ter c.p. — Frode informatica e circostanze aggravanti ad effetto speciale

Art. 615-ter c.p. — Accesso abusivo ad un sistema informatico o telematico

Art. 646 c.p. — Appropriazione indebita e requisiti di previo possesso

Art. 192 c.p.p. — Valutazione della prova e requisiti della prova indiziaria

Art. 521 c.p.p. — Correlazione tra l'imputazione contestata e la sentenza

Art. 522 c.p.p. — Nullità della sentenza per difetto di contestazione

Art. 27 Cost. — Presunzione di non colpevolezza e personalità della responsabilità penale

Art. 111 Cost. — Principi del giusto processo, parità delle parti e diritto di difesa

Giurisprudenza citata

1. **Cassazione Penale, Sez. II, sentenza 9 luglio 2026, n. 25792** — Nozione di identità digitale estesa all'home banking, contestazione in fatto dell'aggravante e massima di esperienza sull'accredito bancario.
2. **Cassazione Penale, Sezioni Unite, sentenza 18 maggio 2017, n. 41210** — Accesso abusivo a sistema informatico per finalità ontologicamente estranee a quelle d'ufficio (Savarese).
3. **Cassazione Penale, Sez. V, sentenza 2 marzo 2026, n. 8215** — Abusività dell'accesso a sistema informatico per finalità estranee alla funzione pubblica esercitata.
4. **Cassazione Penale, Sez. II, sentenza 19 marzo 2026, n. 10525** — Struttura materiale della frode informatica e consumazione con il conseguimento dell'ingiusto profitto.

5. **Cassazione Penale, Sez. VII, ordinanza 3 luglio 2026, n. 25203** — Concorso tra accesso abusivo a sistema informatico aziendale e delitto di tentata estorsione.

6. **Cassazione Penale, Sez. II, sentenza 27 ottobre 2022, n. 40862** — Applicabilità dell'aggravante dell'identità digitale alle piattaforme informatiche private di home banking.

7. **Cassazione Penale, Sez. VI, sentenza 28 maggio 2026, n. 22606** — Validità della contestazione in fatto delle circostanze aggravanti e garanzia dell'esercizio del diritto di difesa.

8. **Cassazione Penale, Sez. I, sentenza 26 marzo 2026, n. 19861** — Rispetto del principio di correlazione tra accusa e sentenza ex art. 521 c.p.p. nella contestazione fattuale.

9. **Cassazione Penale, Sez. II, sentenza 18 dicembre 2019, n. 15999** — Requisiti di precisione e determinatezza della contestazione in fatto delle circostanze aggravanti.

10. **Cassazione Penale, Sez. V, sentenza 21 gennaio 2025, n. 4767** — Autoevidenza del fatto materiale e assenza di implicazioni valutative nella rubrica imputativa.

11. **Cassazione Penale, Sez. II, sentenza 24 aprile 2026, n. 14918** — Integrazione dell'aggravante del furto d'identità digitale anche per credenziali previamente carpite da terzi ignoti.

12. **Cassazione Penale, Sez. II, sentenza 23 aprile 2026, n. 16493** — Struttura della frode patrimoniale e normalità causale tra profitto percepito e condotta concorsuale.

13. **Cassazione Penale, Sez. II, sentenza 9 aprile 2026, n. 15091** — Presunzione di responsabilità concorsuale legata all'accredito bancario e onere di allegazione difensiva.

14. **Cassazione Penale, Sez. II, sentenza 30 gennaio 2020, n. 6734** — Principio di vicinanza della prova nel processo penale ed oneri di allegazione a carico dell'imputato.

Dottrina richiamata

D1. Metodo Giuridico, *Confisca per equivalente e proporzionalità reale nel sequestro penale*. Analisi delle misure ablative reali e tutela patrimoniale del reo.

D2. Metodo Giuridico, *Autoriciclaggio e reati presupposto: la motivazione effettiva della condotta decettiva*. Studio sui flussi patrimoniali complessi e imputazione soggettiva.

Redazione di Metodo Giuridico

Rivista di Diritto e Giurisprudenza

A cura della Redazione di Metodo Giuridico, rivista scientifica specializzata in Diritto e Giurisprudenza.