Rosa Maria Vadalà

LA TUTELA PENALE DELLA SICUREZZA DEGLI **SCAMBI ECONOMICI DIGITALI**

Rosa Maria Vadalà

Pubblicato solo on line

Formato ebook

Università degli Studi di Verona

Dipartimento di Scienze Giuridiche

Via Carlo Montanari, 9 – 37122 Verona (Italia)

ISBN 9788899957025

Alla perseveranza che rende possibile ogni cosa

Indice Sommario

Capitolo I

Riflessi penali della digitalizzazione economica

Capitolo II

La consistenza delle valute virtuali

Capitolo III

Gli obblighi d'incriminazione della direttiva UE/2019/713

Capitolo IV

La tutela penale delle valute virtuali nell'ordinamento nazionale

Capitolo I

Riflessi penali della digitalizzazione economica

Sommario: 1. Ambientazione fenomenologica; 2. Prime indicazioni di analisi, 3.La prospettiva degli scambi, 4. Alla ricerca di un patrimonio anche digitale.

1. *Ambientazione fenomenologica*

La repressione penale degli attacchi al patrimonio deve fare i conti con una realtà economica finanziaria lontanissima da quella che aveva costituito il sostrato sostanziale dei delitti contro il patrimonio nel codice Rocco[1].

Fino a qualche anno fa lo studioso era chiamato ad affrontare le prime sfide della globalizzazione[2].

Oggi questa prospettiva può dirsi amplificata in quanto "*l'applicazione di sofisticati modelli legati all'utilizzo di macchine automatizzate ha dato impulso ad una dimensione planetaria dell'economia, fondata sulla libera circolazione dei capitali e sulla possibilità di attuare investimenti senza frontiere*"[3].

Questa dimensione planetaria si è affermata grazie a quella inter-connettività resa possibile dallo sviluppo delle tecnologie dell'informazione e della comunicazione (c.d. TIC) e in generale dall'avvento d'Internet[4].

La prospettiva digitale segnalata ha, in particolare, inciso sul sistema economico, non solo individuando nuovi canali e sbocchi, ma di fatto mutandone anche i poli d'attrattiva degli operatori, sempre più interessati all'acquisizione dei dati che gli utenti immettono nella rete: "*gusti, inclinazioni, opinioni, relazioni dell'utente sono costantemente monitorate e acquistano un enorme valore commerciale*"[5].

---

[1] Sul punto SGUBBI, voce *Patrimonio (reati contro il),* in *Enc. Giur.*, XXXII, 1982, p. 331 ss.; PECORELLA, voce *Furto*, in *Enc. dir.*, XVIII, 1969, p. 313 ss.; CARMONA, *Tutela penale del patrimonio individuale e collettivo*, Mulino, 1996, p. 13 discorre di un asseto codicistico dei reati contro il patrimonio conforme ad una società prevalentemente agricola e concepito secondo una visione liberistica ottocentesca.

[2] Discorre di "*globalizzazione economica e integrazione sovranazionale*" come "*moltiplicatori del processo espansivo dello ius criminale*" MONGILLO, *Il contrasto alla corruzione tra suggestioni del "tipo d'autore" e derive emergenziali*, in *Rivista Italiana di Diritto e Procedura Penale*, 2/2020, p. 983; sulla dinamica in generale di "*ridefinizione degli ordinamenti costituzionali contemporanei in relazione alle dinamiche della globalizzazione*" vedi anche MILITELLO, *L'identità della scienza giuridica penale nell'ordinamento multilivello*, in *Rivista Italiana di Diritto e Procedura Penale*, 1/2014, p. 106.

[3] Così MIGLIONICO, *Innovazione tecnologica e digitalizzazione dei rapporti finanziari*, in *Contratto e Impr.*, 4/2019, p. 1376 nota 4.

[4] Per un quadro generale di questa evoluzione fino alla cybernetic revolution cfr. PICOTTI, *New technologies as tool and means against crime: substantive aspects*, in SEVERINO, VERVAELE, GULLO (a cura di), *Criminal Justice and Corporate Business, 20th AIDP International Congress of Penal Law, Rome, Italy, 13th-16th November 2019*, Muklu Publishers, 2021, p. 183-186.

[5] CUNIBERTI, *Tecnologie digitali e libertà politiche*, in *Diritto dell'Informazione e dell'Informatica, 2/2015,* p. *277-278.*

Mediante strumenti di analisi informatica e algoritmica di questi dati, quali espressione digitale dei comportamenti umani, è, infatti, possibile estrapolare informazioni che non solo possono essere sfruttate economicamente dalle imprese per l'individuazione di conformi prodotti e servizi, ma direttamente commercializzate in apposite piattaforme, cd. *data marketplace*[6]. Si assiste così accanto ad una digitalizzazione del patrimonio ad un processo di "patrimonializzazione dei dati", che genera interrogativi sulla portata e sui contenuti della loro tutela[7].

Espressione rilevante di questa *Big data economy*[8] è l'evoluzione FinTech[9]: "*dati di quantità e qualità elevate non sono un mero fattore di facilitazione dei processi di digitalizzazione della prestazione dei servizi finanziari, ma un vero e proprio requisito di operatività*"[10].

Il riferimento a questo fenomeno va qui, in particolare, inteso quale "*eterogeneo ecosistema, che racchiude diverse articolazioni o fattispecie, più o meno diffuse sul mercato, accomunate dal fatto di essere considerate as financial activities which provide an added value by means of digital technology*"[11]: "*dalla creazione di nuovi sistemi di pagamento, ai canali di finanziamento alternativi; dalla creazione di nuove valute virtuali sino ai nuovi processi attraverso i quali vengono offerti servizi finanziari già conosciuti*"[12].

---

[6] MAGGIOLINO, SCOPSI, *Big data e profili di concorrenza nei mercati dei servizi bancari e finanziari*, in BOSCIA, SCHIENA, STEFANELLI (a cura di), *Digital Banking e Fin tech. L'intermediazione finanziaria tra cambiamenti tecnologici e sfide di mercato*, Bancaria editrice, 2020, p. 90.

[7] In questi termini e specificatamente di proprietarizzazione dei dati personali inseriti in una piattaforma di *lending* o *crowdfunding* v. MORGANTE, AMORE, VETTA, FIORINELLI, GALLI, *Enforcement e regimi sanzionatori tra rischi per la clientela e vincoli per gli operatori: i profili penalistici*, in CONSOB (a cura di), *Il FinTech e l'economia dei dati. Considerazioni su alcuni profili civilistici e penalistici. Le soluzioni del diritto vigente ai rischi per la clientela e gli operatori*, nella collana *Quaderni FinTech* n. 2/2018, p. 48.

[8] Sulla definizione di Big data come "*insieme di dati che per la loro estensione in volume, velocità e varietà consentono di estrarre informazioni aggiuntive sui soggetti da cui provengono, rendendo obsolete le tradizionali tecnologie di conservazione ed elaborazione dei dati medesimi. (….). I dati in sé non hanno valore; l'elaborazione di set massivi di dati in forma di Big data conferisce loro un valore. Da qui, la più importante caratteristica dei Big data, ossia la V di "valore""* si rinvia a MENZELLA, *Il ruolo dei big data e il mobile payment*, in MAIMERI, MANCINI (a cura di), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale*, Quaderno di ricerca giuridica della Banca d'Italia, n. 87/2019, p. 148.

[9] Sulla definizione e la descrizione delle fasi di sviluppo di Fin Tech o *Financial Technology*, quale la fornitura di servizi e prodotti finanziari in senso ampio mediante le tecnologie dell'informazione (ICT), si rinvia a FIMMANÒ, FALCONE, "*FinTech": scenari, soggetti, temi*, in FIMMANÒ, FALCONE (a cura di), *FinTech*, Edizioni scientifiche Italiane, 2019, p. 1 ss..

[10] Testualmente FIMMANÒ, FALCONE, "*FinTech": scenari, soggetti, temi*, cit., p. 2

[11] Così SERAFIN, *FinTech: tra piattaforme di crowdfunding, valute virtuali e contrasto del riciclaggio*, in *Ricerche giuridiche*, vol. 8, n. 1/2019, p. 121 e nota 5.

[12] Testualmente SERAFIN, *op. ult. cit.*. Possono essere considerati servizi innovativi quelli del *marketplace lending* e della *supply chain finance*, rispettivamente di finanziamento a medio-lungo periodo e breve periodo, tra cui collocare l'equity crowdfunding e il lending crowdfunding, differenziati in base all'assunzione o meno da parte della piattaforma di posizioni creditorie. Per un'analisi tecnica di questi istituti si rinvia a BOSCIA, STEFANELLI, SAPRIO, *L'impatto delle digital technologies nei processi di finanziamento: le risposte della banche incumbents e delle FinTech*, in BOSCIA, SCHIENA, STEFANELLI (a cura di), *Digital Banking e Fin tech. L'intermediazione finanziaria tra cambiamenti tecnologici e sfide di mercato, cit.*, p. 212-222. Nella medesima opera per l'esame di servizi già noti di e-payments, quale carte di credito o di debito utilizzabile via internet, o di mobile payments fino alle forme più evolute di *voice* ed *instant payments* e delle valute virtuali si rinvia a BOSCIA, STEFANELLI-

Come è stato icasticamente sintetizzato, blockchain, piattaforme informatiche, algoritmi sono "*la triade dalla quale si dipartono le diverse esperienze che si chiamano monete virtuali, transazioni di pagamento peer to peer, operazioni di raccolta (si pensi al crowdfunding) e di impiego (il peer to peer lending)*"[13].

Queste nuove realtà si caratterizzano non solo per la disintermediazione degli scambi[14], ma anche per la loro anonimizzazione[15]: grazie, ad esempio, all'impiego di *robo-advisor*[16] nella consulenza finanziaria o all'affidamento agli algoritmi di *High Frequency Trading* nelle scelte delle operazioni di acquisto e vendita sui mercati finanziari[17], il fattore umano della relazione commerciale rischia di essere rimpiazzato da quello tecnologico.

I profili sinteticamente accennati permettono di cogliere la carica dirompente dell'evoluzione FinTech, la quale costituisce un fattore di accrescimento della rivoluzione cibernetica poiché, generando nuovi operatori, nuovi processi e nuovi prodotti[18], impedisce che il rapporto tra servizi bancari-finanziari e TIC sia predicabile in termini meramente strumentali[19].

2. *Prime indicazioni di analisi.*

VERGALLO-CAIONE, *Le innovazioni tecnologiche digitali nei servizi di pagamento: tra instant payments e voice banking*, p. 184-197.

[13] Così MAIMERI, MANCINI, nell'introduzione all'opera da loro curata, *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale, cit.*, p. 17.

[14] Sul punto e sulla connessa operatività dei canali distributivi telematici "cross border" si rinvia a SCHENA, TANDA, ARLOTTA, *Lo sviluppo del FinTech. Opportunità e rischi per l'industria finanziaria nell'era digitale*, in *Quaderno Fin Tech*, 1/2018, p. 15.

[15] Nel senso dell'anonimizzazione delle relazioni MIGLIONICO, *Innovazione tecnologica e digitalizzazione dei rapporti finanziari*, *cit.*, p. 1377.

[16] Sulla definizione di robo-advisor quale agente finanziario virtuale nel senso che la consulenza finanziaria è interamente gestita mediante ricorso alla tecnologia, dall'analisi del portafoglio alle scelte d'investimento, si rinvia a CUCURACHI, *Lo sviluppo del FinTech a supporto della consulenza finanziaria agli investitori*, in BOSCIA, SCHIENA, STEFANELLI (a cura di), *Digital Banking e Fin tech. L'intermediazione finanziaria tra cambiamenti tecnologici e sfide di mercato, cit.*, p. 226 ss. Vedi, anche, per una ricognizione sull'offerta di consulenza automatizzata in Italia e sulla sua specialità rispetto al quadro normativo esistente CONSOB, *La digitalizzazione della consulenza in materia di investimenti finanziari*, in *Quaderno Fin Tech*, 3/2019, p. 7 ss.

[17] Sulla definizione generale di negoziazione algoritmica e specificatamente su quella di *high frequency trading* si rinvia a LUCANTONI, *Strumenti digitali e finanza,* in MAIMERI, MANCINI (a cura di), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale*, *cit.*, p. 295-297, il quale evidenzia come il loro impiego possa provocare pericolose reazioni a cascata per la stabilità dei mercati e la sicurezza dei loro partecipanti e come mediante gli stessi il trading on line si decaratterizzi dall'intermediario che lo predispone.

[18] MENZELLA, *Il FinTech e le regole (una, nessuna o centomila?),* in FIMMANÒ, FALCONE (a cura di), *FinTech*, *cit.*, p. 47.

[19] In questo senso e sulla capacità dell'evoluzione FinTech di "riconfigurare" il mercato finanziario, i suo attori, le sue regole e le stesse modalità e strutture delle attività di vigilanza che su quel mercato e su quei soggetti andrà dispiegandosi v. FIMMANÒ, FALCONE, *op. ult.* cit..

Gli elementi di novità ed anzi di rottura[20] rispetto ai sistemi e al comportamento degli operatori economico-finanziari tradizionali richiedono interventi regolamentari[21] capaci di bilanciare le enormi opportunità derivanti dall'evoluzione in atto con la garanzia dell'integrità e sicurezza delle transazioni economiche che avvengono mediante ricorso alle TIC: è indubbio, infatti, che la digitalizzazione genera vantaggi in termini di riduzione dei costi, di concorrenza, di accessibilità[22], ma comporta, sia per l'utente che per l'operatore, anche l'amplificazione di rischi già noti, quali forme di volatilità finanziaria, e la creazione di nuovi, strettamente connessi al contesto digitale in quanto legati alla vulnerabilità dei sistemi[23].

Questa duplice prospettiva è alla base della strategia della Commissione Europea sulla finanza digitale per il 2020-2024, che, da un parte, considera i servizi FinTech quale strumento "*to help repair the social and economic damage brought by the pandemic*"[24], dall'altra, individua quale finalità da perseguire nel 2024 "*continuously empowering and protecting consumers to ensure that they benefit from a broader access, under safe conditions, to innovative products and services. The protection of the public interest against the risk of money laundering, terrorist financing and any other financial misbehaviours including tax evasion should progress in parallel*"[25].

---

[20] DI PORTO, STARITA, *La strategia europea sulla digitalizzazione e il posizionamenti dell'Italia*, in BOSCIA, SCHIENA, STEFANELLI (a cura di), *Digital Banking e Fin tech. L'intermediazione finanziaria tra cambiamenti tecnologici e sfide di mercato*, *cit.*, p. 29. Gli Autori definiscono l'innovazione tecnologica nell'industria bancaria, finanziaria e assicurativa *disruptive* perché ne sta determinando un cambiamento strutturale.

[21] Per la ricostruzione delle linee evolutive dell'approccio regolamentare adottato a livello internazionale, europeo ed italiano con specifico riferimento alle piattaforme di *equity* e *lending crowdfunding* e criptovalute vedi SCHENA, TANDA, *Linee evolutive della regolamentazione e della vigilanza sull'innovazione finanziaria digitale*, in BOSCIA, SCHIENA, STEFANELLI (a cura di), *Digital Banking e Fin tech. L'intermediazione finanziaria tra cambiamenti tecnologici e sfide di mercato*, *cit.*, p. 69-84.

[22] Discorre anche di riduzione di asimmetrie informative e barriere in ingresso, ZONILE, *La regolamentazione internazionale ed europea di contrasto all'uso di valute virtuali da parte della criminalità transnazionale*, in *Rivista di Diritto Internazionale*, 1/2019, p. 138.

[23] MORGANTE, AMORE, DI VETTA, FIORINELLI, GALLI, *Enforcement e regimi sanzionatori tra rischi per la clientela e vincoli per gli operatori: i profili penalistici dell'analisi*, in *Quaderno Fin Tech*, 2/2018, p. 47. Gli Autori ritengono che "*il progressivo sviluppo delle attività di finanza tecnologica ha comportato la singolare convergenza di due distinti profili di rischio per la clientela: accanto, infatti, ai rischi di natura finanziaria cui tali attività sono per natura connesse, la prestazione di servizi mediante strumenti tecnologici introduce inedite istanze di tutela, emergenti direttamente dalla natura digitale ed informatica dell'attività: ciò non soltanto a causa della 'smaterializzazione' delle relazioni tra clientela ed operatori, ma anche – e soprattutto – in conseguenza dell'assoluta rilevanza ora assunta dalla necessità di tutela dei dati*".

[24] Testualmente la Comunicazione della Commissione Europea al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni relativa a una strategia in materia di finanza digitale per l'UE, COM(2020) 591 final del 24.9.2020. Si riporta di seguito l'intero periodo da cui è tratta la citazione nella traduzione ufficiale in italiano: "*Nel contesto della sua strategia di ripresa l'Europa deve trarne il massimo vantaggio, per contribuire a riparare i danni sociali ed economici causati dalla pandemia. Le tecnologie digitali saranno essenziali per rilanciare e modernizzare l'economia europea in tutti i settori. Permetteranno l'avanzamento dell'Europa come attore digitale a livello mondiale. Allo stesso tempo, gli utenti dei servizi finanziari devono essere protetti dai rischi provenienti dal maggior ricorso alla finanza digitale*".

[25] Sulla base della Comunicazione di cui alla nota 24, la Commissione intende realizzare l'obiettivo strategico di puntare sulla finanza digitale per il bene di consumatori ed imprese attraverso quattro priorità, che guideranno la sua azione e che possono essere così sintetizzate: 1. il superamento della frammentazione del

E', infatti, incontestabile che le misure sul distanziamento sociale nel contesto pandemico da Covid-19 abbiano accelerato la traslazione dell'operatività economica e sociale sui canali telematici, mettendo in risalto la centralità del "*Cyberspace, quale realtà non solo tecnologica, ma di assorbente interazione, scambio e comunicazione permanente, fra qualsivoglia soggetto ed ente, pubblico e privato*"[26].

Questa accelerata virata è stata, però, accompagnata dall'incremento di reati via web, quali frodi e attacchi informatici contro privati ed istituzioni pubbliche, truffe, clonazioni di carte di credito, *phishing* e furti di identità digitale[27].

Quanto sopra ha contribuito all'acquisizione che lo sviluppo della finanza digitale deve realizzarsi congiuntamente a quello di adeguati livelli di protezione dell'"*integrità e sicurezza informatica*"[28].

Tra gli obiettivi della citata strategia della Commissione non è un caso che sia stato previsto proprio il "*Reinforcement of digital operational resilience of financial market participants (…)The EU cannot afford to have the operational resilience and security of its digital financial infrastructure and services called into question. There is also a need to minimise the risk of client funds being stolen or their data compromised*"[29].

---

mercato unico digitale nell'ambito dei servizi finanziari; 2. la creazione di un quadro normativo dell'UE che agevoli l'innovazione digitale nell'interesse dei consumatori e dell'efficienza del mercato; 3. la costituzione di uno spazio europeo di dati finanziari al fine di promuovere l'innovazione guidata dai dati; 4. il controllo dei rischi legati alla trasformazione digitale. Rientra nell'ultima priorità la finalità testualmente riportata "*di conferire un ruolo attivo ai consumatori e di proteggerli costantemente, affinché possano beneficiare di un accesso più ampio a prodotti e servizi innovativi in condizioni di sicurezza. La tutela dell'interesse pubblico dal rischio di riciclaggio di denaro, finanziamento del terrorismo e altri tipi di condotte finanziarie illecite, inclusa l'evasione fiscale, dovrebbe procedere in parallelo*".

[26] In questi termini PICOTTI, *Cybersecurity: quid novi?,* in *Diritto di Internet*, 1/2020, p. 12.

[27]In proposito il comunicato stampa del Sisr, Sistema per l'informazione e la sicurezza della Repubblica, del 1 aprile 2020, consultabile nella sezione notizie del sito *www.sicurezzanazionale.gov.it*, e i risultati del servizio di analisi criminale che fa capo alla direzione centrale della Polizia, consultabile al seguente link *https://www.ilsole24ore.com/art/i-furti-e-rapine-crollano-il-virus-ma-piu-reati-web-AD7B5Px*. Un trend analogo è stato rappresentato da Moneyval, l'organo preposto alle politiche antiriciclaggio nell'ambito del Consiglio d'Europa, nella sua attività di *mutual evaluation* dei Paesi membri in cui applica gli standard e la metodologia del GAFI, in particolare con il report *Money laundering and terrorism financing trends in MONEYVAL jurisdictions during the COVID-19 crisis*, 2 settembre 2020, consultabile alla pagina *www.coe.int/moneyval*, è stata tracciata la seguente evoluzione criminale: *"There was no reported increase in crimes related to drug trafficking, terrorist financing, abuse of NPOs and insider trading. On the other hand, several jurisdictions highlighted instances where medicrime, cybercrime and corruption grew. 10. All jurisdictions noted a significant and rapid growth in the number of frauds related to COVID-19 and the adaptation of well-known fraud to the new (confined and more remote) lifestyle of individuals and businesses. 11. Despite the economic downturn, illicit financial flows continue to run, criminals seeking to exploit temporary weakness in AML/CTF controls of financial institutions (FIs), designated non-financial businesses and professions (DNFBPs) and virtual asset service providers (VASPs). Due to the financial standstill caused by preventing further spread of COVID-19 pandemic there is a risk that AML/CFT measures will be relaxed or considered less of priority in order to boost the economy and expedite process of payments. 12. Five main categories of potential ML threats emerged from the replies to the survey: (i) fraud, (ii) medicrime, (iii) corruption and (iv) cybercrime, and (v) late demand in moving illicit funds."*

[28] Per l'emersione, in conseguenza dell'applicazione dell'informatica ai rapporti economici e sociali, del bene giuridico dell'"integrità e sicurezza informatica" quale nuovo interesse meritevole di tutela penale, PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, Cedam, 2004, p. 70.

[29] Testualmente la Comunicazione della Commissione relativa a una strategia in materia di finanza digitale per l'UE, *cit*., nella quale si dà atto che questo obiettivo viene perseguito mediante la Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo alla resilienza operativa digitale per il settore finanziario e

Come emerge dal citato obiettivo, la prevenzione e repressione delle aggressioni patrimoniali perpetrabili in connessione agli innovativi servizi economici-finanziari FinTech passa anche attraverso la garanzia della sicurezza informatica da parte di chi li eroga.

Nella consapevolezza di questo assunto, si tenterà di tracciare i connotati identificativi della risposta penale sia a protezione dell'uso, sia a repressione dell'abuso delle valute virtuali.

Non si intende semplicemente individuare le possibili fattispecie vigenti applicabili, evidenziandone i limiti e proponendone le modifiche ritenuto opportune, ma tracciare altresì le coordinate della tutela penale degli scambi digitali ed in particolar modo degli interessi soprattutto patrimoniali di coloro che intendono avvalersi di questi servizi.

L'analisi di questi profili con riferimento ai servizi FinTech vuole essere l'occasione per l'individuazione di paradigmi punitivi che possano fungere da indicazioni per un inquadramento sistematico.

3. *La prospettiva degli scambi*

Nella direzione d'indagine delineata il riferimento agli scambi non ha una mera valenza linguistica, ma connota il senso della loro idoneità a rappresentare l'essenza multiforme ed attuale dell'economia finanziaria globale.

La centralità della relazione di scambio, quale nota identificativa anche del corrispondente regime penale, è stata colta da quella dottrina che, con riferimento al commercio elettronico e ai servizi finanziari, ha parlato di un "*diritto penale delle relazioni negoziali, comprendente tutti i diversi stadi di intervento del magistero punitivo a presidio della correttezza delle contrattazioni e a garanzia dell'inclusione finanziaria e digitale di un contraente reso vieppiù debole in ragione del prodotto e del processo contrattuale*".[30]

Secondo questa visione, il fattore unificante sarebbe la tutela del contraente debole e nello specifico del suo patrimonio, a presidio del quale sarebbero poste sia le disposizioni che hanno una proiezione immediata e diretta sul contratto, sia quelle a garanzia della correttezza e trasparenza del mercato, nonché quelle che ne condizionano l'accesso, mediante riserve di attività[31].

---

che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014 e (UE) n. 909/2014 (COM(2020) 595 final).

[30] MORGANTE, FIORINELLI, *Sul diritto penale delle relazioni negoziali complesse: la tutela della parte "vulnerabile" tra contratto e mercato*, in *www.discrimen.it* del 24.6.20, p. 3.

[31] MORGANTE, FIORINELLI, *Sul diritto penale delle relazioni negoziali complesse: la tutela della parte "vulnerabile" tra contratto e mercato*, *cit.*, p. 4, per cui le "*diverse riserve di attività penalmente sanzionate" sarebbero poste a tutela della stabilità del sistema," ma anche, di riflesso, del patrimonio dei singoli, sia pur inteso in un'accezione dinamica e collettiva. Su di un piano più generale, dunque, pare attualmente in corso un processo di progressiva de-patrimonializzazione della tutela penale a fronte della dematerializzazione delle negoziazioni contrattuali, in una interessante prospettiva di anticipazione della soglia dell'intervento punitivo che prescinda, in una materia, come anticipato, sempre più connotata dalla vulnerabilità del contraente "non addetto ai lavori", dall'attualità della deminutio patrimonii*".

Una ricostruzione di questo tipo è condizionata dalla identificazione del patrimonio nella sua dimensione evolutiva-dinamica, quale risparmio-investimento costituzionalmente rilevante[32]: in conseguenza della finanziarizzazione della ricchezza[33], la "*moltiplicazione dei diritti delle possibilità*"- generata dalle "*infinite ragioni di scambio sui mercati- ormai inanimato perché telematico*"- avrebbe fatto del rischio l'oggetto stesso del contratto[34], elevando gli interessi delle parti ad interesse diffuso dei risparmiatori da preservare colmando le asimmetrie informative[35].

Una visione di questo tipo attribuisce al bene giuridico patrimonio carattere superindividuale, rendendo, però, evanescenti i confini con altri beni di stampo pubblicistico, quale l'economia pubblica[36], a sua volta interessata invece da un processo di individualizzazione[37]. In questo modo si cerca di proiettare sul piano dogmatico l'evoluzione del sostrato economico di riferimento, in cui la vicenda del singolo è influenzata da quella degli altri in un sistema di scambio massificato e interconnesso globalmente[38].

Pur non condividendo la indifferenziazione o comunque sovrapposizione di piani di tutela che ne consegue, concezioni di questo tipo rilevano come la suddivisione tra regime penale della ricchezza

---

[32] CARMONA, *Tutela penale del patrimonio individuale e collettivo*, *cit.*, p. 251-252, che si riferisce ad una nozione di risparmio quale bene polifunzionale che assume le forme dell'investimento e la cui tutela è funzionale al benessere collettivo.

[33] In questi termini già PEDRAZZI, *Mercati finanziari (disciplina penale),* in *Dig. Disc. Pen.,* Vol. VII, Torino, 1993, p. 654 ss., da cui discende la configurazione del patrimonio come investimento con conseguente copertura costituzionale da parte dell'art. 47 cost..

[34] In questi termini PIERGALLINI, "*Civile" e "penale" a perenne confronto: l'appuntamento di inizio millennio*, in *Riv. it. dir. e proc. pen.*, 2012, 4, p. 1306.

[35] PIERGALLINI, "*Civile" e "penale" a perenne confronto: l'appuntamento di inizio millennio*, *cit.*, p. 1308-1309. Nel senso anche "*dell'impossibilità di scindere la tutela dell'integrità del sistema finanziario (o del mercato o del risparmio) – quale bene collettivo –dalla tutela dell'investitore"* per cui nel "*contenitore della tutela dell'integrità del mercato si racchiudono un numero infinito di posizioni individuali, il cui interesse alla massimizzazione del profitto si traduce nell'interesse alla migliore allocazione delle risorse economiche. In sostanza, nel fuoco di tutela della truffa contrattuale entrano, accanto ad interessi individuali, anche interessi generali come quello della tutela della libertà degli scambi commerciali, la fiducia in un mercato integro, affidabile e trasparente, la buona fede nelle transazioni e nelle relazioni con gli intermediari e istituti bancari*" v. MAGRO, *Truffa contrattuale e derivati: profilazione dell'investitore e standard di tutela penale*, in *Cassazione Penale*, 2015/9, p. 3355B ss..

[36] In questo senso PEDRAZZI, *La riforma dei reati contro il patrimonio e contro l'economia, in AA.VV., Verso un nuovo codice penale. Itinerari. Problemi. Prospettive, Atti del Convegno di Palermo del 7-10 novembre 1991*, Milano, 1993, p. 352. Nel senso che la distinzione tra i reati contro il patrimonio e quelli contro l'economia pubblica è divenuta fluida e confusa v. BERTOLINO, *Nuovi orizzonti dei delitti contro il patrimonio nella circonvenzione di incapace e nell'usura*, Giappichelli, Torino, 2010, p. 20.

[37] Testualmente GIUNTA, *Lineamenti di diritto penale dell'economia, Delitti contro l'economia pubblica e reati societari*, Vol. I., II ed., Giappichelli, 2004, Torino, p. 58, secondo cui "*la dimensione economica dell'offesa si interseca con il pregiudizio che il fatto incriminato arreca (o può arrecare) ad interessi patrimoniali individuali*" con conseguente qualificazione come reato economico di quelle condotte pregiudizievoli di interessi patrimoniali individuali che siano anche diffusi.

[38] CARMONA, *op. cit.*, p. 246, che fa riferimento, quale risvolto di questa interconnessione, all'attacco patrimoniale che si espande dal singolo rapporto individuale ad interessi collettivi.

statica-individuale e quello della ricchezza dinamica-collettiva[39] sia inadeguata a captare la realtà della consistenza assiologica delle relazioni.

Limitando l'analisi alle sole fattispecie codicistiche questa suddivisione ha, infatti, perso la sua funzione di identificazione rispettivamente dei delitti contro il patrimonio e di quelli contro l'economia, non essendo in grado di differenziare, né all'esterno, né all'interno, i delitti dei titoli VIII e XIII, libro II del codice penale[40].

Questa crisi della predetta suddivisione categoriale deriva, anche, dal carattere anacronistico della nozione di riferimento di "economia pubblica" adottata dal titolo VIII, in conseguenza del quale esso individua, di fatto, "*le aggressioni al sistema economico nazionale statisticamente meno frequenti e, ad un tempo, più elementari, in quanto tipiche espressioni di una concezione paleocapitalistica dell'economia*"[41].

Con riferimento, invece, ai delitti del titolo XIII, la difficoltà d'individuare un comune denominatore sarebbe stata acuita dall'introduzione di reati sempre più proiettati verso ulteriori e ultronee finalità di tutela[42], con la conseguenza che la "*fisionomia codicistica della tutela patrimoniale risulta attualmente proteiforme con elementi "vecchi" e "nuovi" che paiono meramente giustapposti*"[43].

A conferma della predetta deriva assiologica, un insigne studioso, oltre trent'anni fa, aveva diviso i delitti del titolo XIII c.p. in reati contro il patrimonio in senso stretto e quelli, costituenti la maggioranza, plurioffensivi in cui "*l'offesa a beni diversi dal patrimonio (la libertà personale, l'amministrazione della giustizia) si accentua fortemente, offuscando la lesione patrimoniale*" [44].

---

[39] La nota distinzione si deve a CARNELUTTI *La tutela penale della ricchezza*, in *Riv. it. dir. pen.*, 1931, p. 7.

[40] In proposito BERTOLINO, *Nuovi orizzonti dei delitti contro il patrimonio nella circonvenzione di incapace e nell'usura*, cit., p. 35-36. Per RAMPIONI, *Diritto penale dell'economia*, Giappichelli, Torino, 2016, p. 7, il titolo VIII del Libro II è espressione della visione corporativa dello Stato e della società civile dell'epoca, costituente "*un quadro normativo, dunque, non in grado di incidere sulla realtà pratica, essendo costituito da figure criminose o poste a tutela di beni di dimensioni talmente grandi (il sistema economico nella sua globalità, le risorse produttive nazionali) da risultare irraggiungibili dalle diverse modalità di aggressione tipizzate ovvero incentrate su un'offesa (evento o messa in pericolo) in fatto non verificabile e non suscettibile di accertamento probatorio*".

[41] Testualmente GIUNTA, *Lineamenti di diritto penale dell'economia*, *cit.*, p. 64.

[42] Con riferimento alla "depatrimonializzazione" dell'oggettività giuridica tutelata da alcune fattispecie del titolo XIII v. GIUNTA, *Il diritto penale dell'economia: tecniche normative e prova dei fatti*, in *Riv. trim. dir. pen. econ.* 3-4/2017, p. 50.

[43] Testualmente FORMICA, *Introduzione. I reati contro il patrimonio*, in VIGANÒ, PIERGALLINI (a cura di), *Reati contro la persona e contro il patrimonio*, II ed. Giappichelli, 2015, Torino, p. 378.

[44] Così SGUBBI, voce *Patrimonio (reati contro il), cit.*, p. 333, che annovera tra le fattispecie tradizionalmente considerate plurioffensive la rapina, l'estorsione, il sequestro di persona a scopo di estorsione e la ricettazione e ritiene che "*esse si collocano fuori del sistema, essendo governate da princìpi propri ed autonomi, eterogenei in confronto a quelli caratteristici dei reati contro il patrimonio*".

Le vicende normative interessanti in particolare i delitti di usura[45], di truffa aggravata per il conseguimento di erogazioni pubbliche[46], di riciclaggio[47], d'impiego e di autoriciclaggio[48] hanno avvalorato questa tesi: la proiezione verso altre finalità di tutela è percepibile per questi delitti già sul piano della stessa tecnica di definizione del fatto tipico, sempre più lontana da quella, propria delle aggressioni patrimoniali, di definita modalità di lesione[49].

---

[45] BERTOLINO, *Nuovi orizzonti dei delitti contro il patrimonio nella circonvenzione di incapace e nell'usura*, cit., p. 102-103, secondo cui il bene tutelato è costituito dal mercato del credito, offeso dalla realizzazione di un'operazione difforme dai parametri legali a prescindere ed indipendentemente da forme di compromissione dell'autonomia decisionale della vittima.

[46] Si veda in questo senso e sull'origine e discussa natura di questa fattispecie PELISSERO, *Truffa aggravata per il conseguimento di erogazioni pubbliche*, in *Riv. it. dir. proc. pen*., 1991, p. 923 ss.; TERRACINA, *La truffa aggravata per il conseguimento di erogazioni pubbliche ed il ruolo del bene giuridico nella fattispecie di reato*, in *Indice penale*, 2/2003, p. 667 SS.; FERRARI, *Sui rapporti fra l'indebita percezione di erogazioni a danno dello Stato e la truffa aggravata per il conseguimento di erogazioni pubbliche*, in *Giur. It*., 2004, 3 ss.; MADIA, *Considerazioni in ordine ai rapporti tra l'art. 316 ter c.p. e l'art. 640 bis: quando l'ipertrofia normativa genera disposizioni in tutto o in parte inutili*, in *Cass. pen*., 9/2003, 2680 ss.; PICOTTI, *L'attuazione in Italia degli strumenti dell'Unione europea per la protezione penale degli interessi finanziari comunitari*, in *Riv. trim. dir. pen. econ*., 3/2006, p. 615 ss..

[47] Con riferimento al dibattito mai sopito sul bene protetto da questo reato, ora riferito all'amministrazione della giustizia, ora all'ordine economico in differenti varianti, ora ad entrambe e non solo, v. FLICK, *La repressione del riciclaggio ed il controllo della intermediazione finanziaria. Problemi attuali e prospettive*, in *Riv. it. dir. Proc. Pen*., 1990, p. 1265 ss.; PECORELLA, *Circolazione del denaro e riciclaggio,* in *Riv. It. dir. Proc. Pen*., 1991, p. 1221 ss.; AZZALI, *Diritto penale dell'offesa e riciclaggio*, in *Riv. It. dir. Proc. Pen*., 1993, p. 419 ss.; MOCCIA, *Impiego di capitali illeciti e riciclaggio: la risposta del sistema penale italiano*, in *Riv. It. Dir. Proc. Pen*., 1995, p. 728 ss.; ZANCHETTI, *Il riciclaggio di denaro proveniente da reato,* Giuffre, Milano, 1997, p. 394-295; MORGANTE, *Riflessione su taluni profili problematici dei rapporti tra fattispecie aventi ad oggetto operazioni su denaro o beni di provenienza illecita*, in *Cass. pen.* 1998, p. 2511 ss.; MANGIONE, *Mercati finanziari e criminalità organizzata: spunti problematici sui recenti interventi normativi di contrasto al riciclaggio*, in *Riv. It. Dir. Proc. Pen*., 2000, p 1102 ss.; MANNA, *il bene giuridico tutelato nei delitti di riciclaggio e reimpiego: dal patrimonio all'amministrazione della giustizia sino all'ordine pubblico ed all'ordine economico*, in AA. VV. (a cura di) MANNA, *Riciclaggio e Reati connessi all'intermediazione mobiliare*, Utet, 2000, p. 55 ss.; SEMINARA, *I soggetti attivi del reato di riciclaggio tra diritto vigente e proposte di riforma*, in *Dir. pen. proc*., 2005, p. 241 ss.; PLANTAMURA, *Tipo d'autore o bene giuridico per l'interpretazione e la riforma del delitto di riciclaggio?*, in *Riv. Trim. dir. Pen. econ*., 1-2/2009, p. 161 ss.; COSSEDDU, *Riciclaggio: complessità di un "percorso" normativo*, in *Cass. Pen.,* 2010, p. 3641 ss.; D'ANELLO, *Riciclaggio: dalla tutela penale del patrimonio individuale a quella dell'economia,* in *Archivio penale on line*, n. 2/2012; DELL'OSSO, *Riciclaggio di proventi illeciti e sistema penale*, Giappichelli, Torino, 2017, p. 68-71; VADALÀ, *La provenienza illecita nel delitto di riciclaggio: possibili novità dalla quarta direttiva antiriciclaggio*, in *Riv. Trim. dir. Pen. Econ*., 1-2 2017, p. 234 ss. ; FAZIO, *Cangiante profilo offensivo dei delitti di riciclaggio*, in *www.lalegislazionepenale.eu*, sez. approfondimento del 4.9.2020.

[48] Sull'oggettività giuridica del delitto di autoriciclaggio volendo v. VADALÀ, *L'autoriciclaggio e la soluzione italiana nella recente riforma*, in *Riv. Trim. dir. Pen. Econ*., 3-2015, p. 1916 ss.; CLINCA, *L'incriminazione dell'autoriciclaggio tra tutela dell'ordine economico e garanzie fondamentali*, in www.lalegislazionepenale.eu, sez. approfondimenti del 3.5.2016; LANZI, *La difficile individuazione di limiti applicativi all'autoriciclaggio: il bene giuridico, il tempo e l'oggetto*, in *Indice penale*, 2/2017, n. 2, p. 506 ss.; PALMIERI, *La prevalenza di interessi patrimoniali nella disciplina del riciclaggio e la punibilità dell'autoriciclaggio come simbolica incriminazione del bis in eadem*, in *Indice penale*, 1/2016, n. 1, p. 57 ss.

[49] Per il superamento di questa tecnica con specifico riferimento al delitto di autoriciclaggio v. GIUNTA, *Il diritto penale dell'economia: tecniche normative e prova dei fatti, cit*., p. 551, secondo cui questo reato "*simboleggia il tramonto, anche nel settore economico, del diritto penale chirurgico, caratterizzato dal bisturi dei principi di determinatezza e frammentarietà, a favore del modello del diritto penale chemioterapico rimesso al senso di responsabilità della magistratura, in quanto potenzialmente distruttivo delle cellule malate, di quelle ad esse prossime, ma anche di un congruo numero di cellule sane, sacrificabili in nome dell'efficacia della cura sociale*".

In realtà, anche per altri reati del titolo XIII, meno influenzati dagli sviluppi economici, è possibile cogliere nella loro struttura la protezione d'interessi di tutela che sono estranei all'oggettività giuridica di categoria[50].

La ricostruzione dei contorni di questa oggettività è stata, poi, resa ulteriormente difficile dall'allentamento in sede giurisprudenziale delle maglie del delitto di truffa[51]. Nello specifico, in risposta a tendenze paternalistiche[52] di tutela del contraente ritenuto debole, quale l'acquirente on line[53], è stata ammessa la sussistenza della truffa nella forma aggravata in virtù di automatismi circa la portata ingannevole di certe tecniche di commercializzazione[54]. O ancora, con riferimento all'investitore non professionale, grazie a concezioni peculiari- depatrimonializzate- dei requisiti del

---

[50] Con riferimento al sovvertimento della dimensione patrimoniale originaria nel reato incriminato dall'art. 630 c.p. v. FALCINELLI, *L'atto dispositivo nei delitti contro il patrimonio. Sezioni e intersezioni del sistema penale,* Giappichelli, Torino, 2013, p. 115-117, secondo cui adottando questa prospettiva "*si finisca per sviare l'analisi della fattispecie delittuosa di cui al primo comma dell'art. 630 c.p. in forza della regolamentazione presente nei commi successivi del disposto. Le singole fattispecie e discipline che vi trovano sede possono in effetti dirsi dotate di un diverso spettro offensivo, ben compatibile con la struttura di una autonoma (quand'anche complessa) fattispecie incriminatrice – questa volta sì – lesiva della persona e segnatamente della di lei incolumità: il riferimento è alle ipotesi dei commi 2 e 3*".

[51] Sul punto per la ricostruzione dell'origine di questa tendenza giurisprudenziale con riferimento alla truffa contrattuale v. FANELLI, *La truffa*, Giuffrè, Milano, 1998, p. 75-78, che la contesta in considerazione della circostanza che in questo modo oggetto di tutela della truffa diviene la libertà di contrarre, la quale, invece, è scopo precipuo della tutela civilistica del dolo.

[52] Cfr. MAGRO, *Paternalismo penale e tutela dell'investitore dal rischio finanziario*, in BORSARI, SAMMICHELI, SARRA (a cura di), *Homo Oeconomicus. Neuroscienze, razionalità decisionale ed elemento soggettivo nei reati economici*, *Ius Quid* sez. scientifica, Padova, 2015, p. 195 ss.. Secondo l'Autrice il bisogno generale di sicurezza, di cui è parte la stessa stabilità finanziaria, ha comportato "*il declino del cosiddetto penal welfarism, la fine dell'utopia della riabilitazione e della reintegrazione quale obiettivo razionale della pena e il passaggio da una forma di assistenzialismo penale ad una forma di giustizia penale punitiva e meramente repressiva*"; con specifico riferimento ai servizi finanziari ciò si traduce nell'abbandono del modelli di tutela incentrati sulla trasparenza a favore di "*politiche improntate alla consulenza, la raccomandazione personalizzata e orientata ad una valutazione di appropriatezza delle forme di investimento*", le quali concepiscono "*l'investitore come un soggetto debole che si colloca nella relazione con l'intermediario in modo non paritario, la cui buona fede e fiducia va preservata*".

[53] A titolo esemplificativo e non esaustivo si rinvia sul fenomeno delle truffe su piattaforme di e-commerce MANNA, *Artifici e raggiri online: La truffa contrattuale, il falso informatico e l'abuso dei mezzi di pagamento elettronici*, in *Dir. inf.*, 2002, p. 955 ss.; C. PECORELLA, *Truffe on line: momento consumativo e competenza territoriale,* in *Riv. it. dir. e proc. pen.*, 1/2012, p. 113 ss.; CIPOLLA, *E-commerce e truffa*, in *Giur. merito*, 12/2013, p. 2624 ss.; C. PECORELLA, DOVA, *Profili penali delle truffe on line*, in *Arch. Pen.*, 3/2013, 799 ss.; CAJANI, *Le truffe on line*, in *Diritto penale dell'impresa*, PARODI (a cura di), Giuffrè, 2017, p. 573 ss.; BENEVENTO, *La truffa sussiste indipendentemente dalla prova dell'indisponibilità del bene oggetto di vendita online*, nota a Cass., sez. II, n. 51551/2019, in *Diritto di internet*, n. 2/2020, p. 321 ss..

[54] Per un'applicazione dell'aggravante della minorata difesa nelle vendite on line vedi Cassazione Penale, Sez. II, 14 ottobre 2016 n. 43705, consultabile in www.giurisprudenzapenale.it del 17 febbraio 2017, che riconosce la ricorrenza dell'aggravante sulla base della considerazione che è "*proprio la distanza tra il luogo di commissione del reato, ove l'agente si trova ed il luogo ove si trova l'acquirente del prodotto on line - che ne abbia pagato anticipatamente il prezzo, secondo quella che rappresenta la prassi di simili transazioni - è l'elemento che consente all'autore della truffa di porsi in una posizione di maggior favore rispetto alla vittima, di schermare la sua identità, di fuggire comodamente, di non sottoporre il prodotto venduto ad alcun efficace controllo preventivo da parte dell'acquirente; tutti vantaggi che non potrebbe sfruttare a suo favore, con altrettanta comodità, se la vendita avvenisse de visu*". Per un'analisi critica di questo orientamento si rinvia a LEPERA, *Un caso di reato semplice scambiato per reato circostanziato: sull'improbabile configurabilità dell'aggravante della "minorata difesa" in relazione alle truffe on-line*, in *Cass. pen.*, 2/2017, p. 687 ss..

danno e dell'ingiusto profitto[55], riferiti ai vantaggi/svantaggi derivanti dalla conclusione in sé del contratto, è stato ritenuto sussistente il reato in forza della violazione dei doveri informativi e fiduciari che connotano il mercato finanziario[56].

Ne è derivato che il regime di protezione del patrimonio individuale sia divenuto anche presidio delle "c.*d. regole del gioco, ossia le modalità consentite della competizione tra operatori economici, le quali disegnano la dimensione normativa del mercato. Da questa angolazione il mercato non è soltanto il locus naturalis dominato dalle leggi della domanda e dell'offerta, quanto un locus artificialis, e principalmente giuridico, venendo a coincidere con la regolamentazione delle attività economiche*"[57].

E' testimone di questa circolarità/contiguità di presidi l'affermazione del diritto penale economico "*quale categoria assai ampia di reati contro l'economia in senso lato, dove cioè, accanto all'eventuale o primaria tutela di beni patrimoniali in senso stretto ovvero di beni istituzionali (per es. la tutela dell'attività di vigilanza di un organo di controllo, l'affidabilità del rispetto delle regole del mercato) o funzionali (per es. la trasparenza), si affiancano agli interessi tutelati in via immediata anche beni superindividuali di tipo economico, considerati talora come oggetto, e talaltra anche solo come scopo, anziché oggetto dell'incriminazione*"[58]. In questo modo, come è stato autorevolmente rappresentato, si è assistito ad un avvicinamento, proprio sul piano degli interessi tutelati, tra il diritto penale classico, proiettato sulla protezione d'identificabili beni individuali, e il diritto penale dell'economia, indirizzato verso beni collettivi[59]; si è ritenuto in questa direzione che addirittura le norme poste a tutela del mercato finanziario, quali quelle che reprimono le forme di abusivismo, garantirebbero al risparmiatore/investitore una tutela più incisiva di quella derivante dai tradizionali reati contro il patrimonio[60].

Anche i servizi FinTech sono destinati a confrontarsi con questa prospettiva, nella misura in cui i recenti interventi nazionali e le iniziative sovranazionali spingono verso forme di controllo dei nuovi

---

[55] Sull'identificazione a tale fine del danno con l'utilità soggettiva e conseguentemente dell'ampliamento del profitto, autonomizzato dal dato patrimoniale, v. MARINI, *Delitti contro il patrimonio*, Giappichelli, Torino, 1999, p. 424-429.

[56] In questi termini MAGRO, *Truffa contrattuale e derivati: profilazione dell'investitore e standard di tutela penale*, in *Cass. Pen.*, 9/2015, p. 3362, che evidenzia come la violazione di norme protezionistiche diviene dirimente nella valutazione dell'induzione in errore.

[57] GIUNTA, *Il diritto penale dell'economia: tecniche normative e prova dei fatti*, cit., p. 546.

[58] Testualmente DONINI, *Un nuovo medioevo penale? Vecchio e nuovo nell'espansione del diritto penale economico*, in *Cass. pen.*, 6/2003, p. 1808.

[59] SEVERINO, *Sicurezza dei mercati finanziaria: interessi tutelati e strumenti di tutela,* in *Riv. it. dir. e proc. pen.*, 2/2014, p. 675. In senso analogo anche FIORELLA, *L'economia pubblica e privata quale oggetto dell'offesa e parametro del campo di materia*, in *Riv. trim. dir. pen. econ.*, 3-4/2017, p. 473 per cui "*il bene fondamentalmente e propriamente offeso da molti illeciti del diritto penale dell'economia sembra doversi individuare nel patrimonio dei privati (più o meno diffusamente pregiudicato) piuttosto che nella «pubblica economia» strettamente intesa. La conclusione comporta – si è visto – che, sul piano dell'individuazione del disvalore di evento e del livello dell'offesa al bene giuridico oggetto dello specifico reato, è al patrimonio dei singoli che bisogna guardare. Al medesimo bene occorre far capo per individuare il soggetto passivo del reato ed il titolare dell'azione civile di danno*".

[60] ROSSI, *L'esperienza giurisprudenziale del diritto penale economico nel tempo della crisi,* in *Riv. it. dir. e proc. pen.*, 2/2014, p. 640.

operatori, o mediante l'estensione di obblighi, quali quelli in materia di prevenzione del riciclaggio e del finanziamento del terrorismo[61], o mediante la creazione di appositi regimi prudenziali e di vigilanza ovvero la specificazione di quelli esistenti[62].

In questo modo sembra dirsi superato lo scenario di un sistema disintermediato degli scambi digitali, che si autogoverni e autodisciplini, rilevando invece per il penalista la forma reticolare assunta dal mercato[63] più che altro in termini di emersione di nuovi centri di potere, il cui predominio non è legato tanto alla disponibilità dell'informazione, quanto al controllo dei "dati"[64].

Gli scambi digitali risultano, così, nella molteplicità di occasioni e varietà di oggetto, fattore sia di emersione che di revisione d'interessi degni di rilevanza penale. E che si tratti d'interessi di tipo economico è fuor di dubbio: ma la questione da indagare è se ed a quale nozione di patrimonio come bene giuridico[65] possano essere ricondotti.

---

[61] Con riferimento all'inserimento, mediante il d.lgs. 90/2017 di attuazione della IV direttiva antiriciclaggio, tra gli obbligati antiriciclaggio dei prestatori di servizi "*di conversione di valute virtuali da ovvero in valute aventi corso forzoso*", i c.d. *exchanger*, e dei prestatori di servizi di portafoglio digitale, i c.d. *wallet provider*, definiti come "*ogni persona fisica o giuridica che fornisce, a terzi, a titolo professionale, anche on line, servizi di salvaguardia di chiavi crittografiche private per contro dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali*" (art. 1, comma 2, lett. ff bis), si rinvia a NADDEO, *Nuove frontiere del risparmio, Bitcoin Exchange e rischio penale*, in *Diritto penale e processo*, 1/2019, p. 101 ss.; LUCEV, BONCOMPAGNI, *Criptovalute e profili di rischio penale nelle attività degli exchanger*, in *Giurisprudenza Penale Web*, 2018, 3, p. 1 ss..; INGRAO, *Gli strumenti di prevenzione nazionali ed europei in materia di valute virtuali e riciclaggio*, in *Diritto Penale Contemporaneo Rivista trimestrale*, fasc. 2/2019, p. 159 ss.; volendo anche VADALÀ, *Criptovalute e cyberlaundering: novità antiriciclaggio nell'attesa del recepimento della Direttiva (UE) 2018/1673 sulla lotta al riciclaggio mediante il diritto penale*, in *www.sistemapenale.it* del 6 maggio 2020.

[62] Si segnala che unitamente alla strategia sulla finanza digitale di cui alla nota 24, in data 24 settembre 2020 la Commissione Europea ha presentato, anche, la Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo ai mercati delle cripto-attività e che modifica la direttiva (UE) 2019/1937 (COM/2020/593 final), cd. MiCA. Con questa proposta, in particolare, si prevede l'introduzione di condizioni per l'emissione e l'ammissione alla negoziazione di cripto-attività, nonché di un regime di vigilanza dei fornitori di servizi per le cripto-attività, degli emittenti di token collegati ad attività e degli emittenti di token di moneta elettronica. Nella medesima data è stata anche presentata la Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo ad un regime pilota per le infrastrutture di mercato basate sulla tecnologia di registro distribuito (COM(2020) 594 final), cd. Pilot regime, al fine di esentarle temporaneamente da alcuni requisiti specifici previsti dalla disciplina in vigore in materia di strumenti finanziari che potrebbero impedire lo sviluppo di soluzioni per la negoziazione e il regolamento delle operazioni in cripto-attività diverse da quelle di cui alla proposta MiCa. Sulla base della proposta questo regime pilota dovrebbe consentire, inoltre, alle autorità nazionali competenti e all'autorità europea degli strumenti finanziari e dei mercati (ESMA), che dovranno rilasciare le autorizzazione del caso, di verificare i rischi specifici derivanti dalle cripto-attività e dalle infrastrutture oggetto di applicazione.

[63] In questi termini con riferimento in particolare alle piattaforme di *crowdfunding*, il cui funzionamento sarebbe equiparabile "*più al social network che ai tradizionali siti di e-commerce*" v. MORGANTE, FIORINELLI, *Sul diritto penale delle relazioni negoziali complesse: la tutela della parte "vulnerabile" tra contratto e mercato*, *cit.*, p. 20.

[64] MORGANTE, FIORINELLI, *op. cit.*, p. 22, secondo cui sussiste "*nel contesto del diritto penale delle relazioni negoziali, la necessità di fornire nuove forme di protezione del contraente, che, in un mercato "data-driven", devono mirare alla tutela della trasparenza, della parità di trattamento, dell'inclusione del soggetto nel mercato, del corretto uso dei dati personali, nonché, da ultimo, della sicurezza informatica*".

[65] Non essendo questa la sede per ricostruire la vastità del dibattito dottrinale che ha interessato la categoria del bene giuridico, senza alcuna pretesa di completezza, si rinvia a BRICOLA, *voce Teoria generale del reato*, in *Noviss. Dig. It.*, XIX, 1973, p. 7 ss.; ANGIONI, *Contenuto e funzioni del concetto di bene giuridico,* Giuffrè, Milano,

In via preliminare, nell'affrontare questo quesito, sembra possibile ritenere che il patrimonio possa ancora essere distinto dal differente bene dell'economia.

Come autorevolmente evidenziato "*le odierne esigenze del mercato economico divengono vieppiù incompatibili con le tradizionali tecniche di tutela penale basate su di un interesse giuridico concepito in termini materiali (…) perché la violazione dei nuovi interessi economici non si pone in un mero rapporto quantitativo di maggiore gravità rispetto alla violazione degli interessi patrimoniali tradizionalmente intesi*"[66]. La tutela del mercato e la tutela del patrimonio rimangono, infatti, aree di protezione distinte afferendo la prima alla produzione "professionale"[67] della ricchezza, mentre la seconda al suo possesso e trasferimento.

4. *Alla ricerca di un patrimonio digitale.*

Nel tentare di definire la consistenza assiologica del patrimonio attraverso l'orizzonte performante degli scambi, bisognerà considerarne anche la dimensione digitale non solo per la corrispondente natura dei servizi FinTech, ma per la centralità che il *cyberspace* ha in sé nell'attuale contesto economico ed in generale nell'odierna società e conseguentemente anche nella manifestazione dei fenomeni criminali.

La possibilità di disporre di uno spazio globale, delocalizzato e connotato da istantaneità e operatività continua ha generato e genera un'informatizzazione delle manifestazioni criminali quale risvolto della proiezione nel *cyberspace* del reale[68]. Come autorevolmente rilevato, infatti, "n*on si tratta [infatti] più solo di fronteggiare nuove tipologie di singole condotte, penalmente illecite, definite oggi quali cybercrime, perché costituite da ogni genere di delitti – non solo quelli informatici strettamente intesi – che si possono realizzare in rete (o meglio nel Cyberspace): dall'estorsione, al riciclaggio, dalle truffe e frodi nei*

1983; FIORELLA, *voce Reato in generale*, in *Enc. Dir.*, XXXVIII, Milano, 1987, p. 770 ss.; ZUCCALÀ, *Due questioni attuali sul bene giuridico: la pretesa dimensione "critica" del bene e la pretesa necessaria offesa ad un bene*, in *Riv. Trim. dir. pen. ec.*, n. 3-4/2004, p. 839 ss.; MANES, *Il principio di offensività nel diritto penale. Canone di politica criminale, criterio ermeneutico, parametro di ragionevolezza*, Giuffrè, Torino, 2005; ID., *I recenti tracciati della giurisprudenza costituzionale in materia di offensività e ragionevolezza*, in *Dir. pen. cont.*, 1/2012, 99 ss.; PAGLIARO, *il reato*, Giuffrè, Milano, 2007; MERLI, *Introduzione alla teoria generale del bene giuridico. Il problema. Le fonti. Le tecniche di tutela penale*, ESI, Napoli, 2006; MADIA, *L'impropria" incidenza della teorica del bene giuridico nel dibattito relativo alla nozione di "evento"*, in *Indice penale*, 2/2012, p. 411 ss..

[66] Testualmente FORNASARI, *Il concetto di economia pubblica nel diritto penale. Spunti esegetici e prospettive di riforma*, Giuffrè, Milano, 1994, p. 161.

[67] In questi termini PIOLETTI, *Lex mercatoria e diritto penale*, in *Indice penale*, 2/2017, p. 488.

[68] Diffusamente in proposito e sui conseguenti risvolti criminosi v. FLOR, *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di internet*, in www.penalecontemporaneo.it del 20.12.2012.

mezzi di pagamento, al cyberstalking e cyberbullismo, fino ai più gravi attacchi del cyberterrorism, se non anche del cyberwarfare" [69].

Rispetto al corrispondente reato "comune", quello cibernetico[70] si differenzia non solo per le modalità di manifestazione[71], ma anche per la proiezione offensiva, che appare "rinnovata".

Quanto sopra è particolarmente apprezzabile proprio con riguardo alle forme di aggressione patrimoniale[72], che sono ormai sempre più lontane da meccanismi "predatori" classici[73]: "*se un tempo le aggressioni patrimoniali dovevano compiersi attraverso condotte intrusive nella sfera di dominio fisico altrui, oggi, come si dice spesso: "basta un click" sulla tastiera di un computer o di uno smart phone*"[74].

Questa apparente "semplificazione" modale, che porta, in realtà, con sé complesse questioni applicative e finanche di ridefinizione dogmatica di categorie generali[75], è strettamente dipendente dalla smaterializzazione che connota la ricchezza digitale.

In particolare, nel caso dei servizi FinTech una "cosa" in senso materiale, che si identifichi con il valore scambiato, potrebbe di fatto mai venire ad esistenza, così come interamente spersonalizzata potrebbe essere la stessa interrelazione mediante cui attuare lo scambio, a maggior ragione se realizzato mediante il ricorso a strumenti d'Intelligenza Artificiale.

---

[69] PICOTTI, *Cybersecurity: quid novi?*, *cit*., p. 12.

[70] Cfr. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme,* in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime,* collana *Diritto e procedura penale dell'informatica*, utet, Torino, 2019, p. 78-79, il quale definisce il reato cibernetico in senso ampio quale reato "*in cui la "rete" compare solo quale eventuale o compatibile modalità, oggetto o risultato della condotta costitutiva del "fatto" di reato, che è quindi possibile sussumere anche solo in via interpretativa nella fattispecie base o circostanziata, alla stregua degli elementi che la costituiscono*". L'autore distingue all'interno di questa categoria i reati cibernetici "in senso stretto", in cui, invece, la commissione "in rete" è requisito tipologico o circostanziale normativamente previsto e che sono, infatti, "*logicamente anche "reati informatici in senso stretto", dato che l'elemento che richiede la commissione "in rete" od in Internet o nel Cyberspace implica necessariamente un riferimento esplicito alle TIC. Ma non è vero l'inverso, in quanto non tutti i reati informatici in senso stretto sono anche reati cibernetici in senso stretto, potendo astrattamente l'elemento che richiama le TIC non richiedere necessariamente anche la commissione "in rete", seppur quest'ultima sia l'ipotesi maggiormente ricorrente: ad es. nel caso di frode informatica aggravata dal furto di identità digitale (art. 640-ter, comma 3, c.p.), la commissione potrebbe concepirsi anche in un sistema chiuso, per l'utilizzo abusivo delle credenziali d'accesso ad un computer, che identificano la persona legittimata*".

[71] Nel senso della modifica strutturale delle modalità di realizzazione PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, *cit*., p. 68.

[72]Sulla portata maggiormente lesiva del fatto digitale di aggressione patrimoniale vedi SCOPINARO, *Internet e reati contro il patrimonio*, Giappichelli, 2007, p. 229 la quale discorre con riferimento alla sua repressione, mediante fattispecie ricalcate sul fatto materiale, d'irragionevole equiparazione costituzionalmente illegittima.

[73] LONGOBARDO, *I reati predatori contro il patrimonio*, in *Riv. it. dir. proc. pen*., 2/2020, p. 889 ss.. L'Autore evidenzia come i dati statistici su reati contro il patrimonio con violenza sulle persone e cose evidenziano un trend stabile in diminuzione rispetto al passato, mentre rimangono alti i livelli di allarme sociale e paura, che alimentati dai mass media contribuiscano ad un severa penalità.

[74] Testualmente PAPA, *Future crimes: intelligenza artificiale e rinnovamento del diritto penale*, in *www.discrimen.it* del 4.3.2020, p. 10, che attribuisce la difficoltà di dare forma ad un mondo sempre più smaterializzato, anche, alla proliferazione d'interessi conflittuali meritevoli di tutela.

[75] In questo senso PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, *cit*., p. 80. Specificatamente sull'individuazione del *locus commissi delicti* ad es. delle truffe on line v. FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in CADOPPI , CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime*, *cit*., p. 150-155.

Da quanto sopra deriva la necessità di riferirsi ad una nozione di patrimonio, sganciata dalla materialità del suo oggetto e dalla corporalità del legame che si instaura con il suo titolare.

In questo modo la ricchezza digitale sembrerebbe incentrare la consistenza assiologica del patrimonio sul concetto di valore, che è tale in quanto può essere oggetto di scambio e la cui tutela si sostanzia di fatto nella protezione delle prerogative del suo titolare[76].

Nonostante quanto sopra, ciò non conduce in termini sistematici alla concezione del patrimonio quale bene-mezzo[77] rispetto alla persona, per cui la sua tutela sarebbe declinabile solo ed esclusivamente come utilità da preservare funzionalmente al soddisfacimento dei bisogni materiali e spirituali dei singoli[78].

A parere di chi scrive la centralità della persona nel disegno costituzionale non determina tanto o soltanto una valorizzazione degli impieghi del patrimonio in funzione della sua realizzazione, né tantomeno una mutamento della sua consistenza: la Carta guarda al patrimonio in ogni caso come "fatto economico"[79]. Il vero cambio di prospettiva inaugurato dalla Costituzione sta, in realtà, nel concepirlo non più e solo in maniera "atomistica", quale bene individuale: la qualificazione prescelta è, cioè, di tipo valoriale e dall'angolo di osservazione del suo titolare, quale attore "sociale" che è esposto a limiti e condizionamenti per scopi di tutela collettiva[80] e riceve protezione in conseguenza di quella accordata al risparmio-investimento, quale valore costituzionale ed interesse di tipo pubblicistico[81].

---

[76] In questo senso MAZZANTINI, *La tutela del patrimonio alla prova della smaterializzazione dei rapporti socio-economici. La centralità dei delitti di frode nel sistema penale "vivente"*, in *Riv. it. dir. pen. proc.*, 1/2020, p. 88, per cui anche la smaterializzazione inciderebbe sulla stessa dicotomia uso-titolarità su cui sarebbe stato costruito il sistema codicistico dei reati contro il patrimonio.

[77] In senso favorevole a questa lettura, con abbandono di una concezione di patrimonio come bene-fine, si rinvia a MILITELLO, *voce Patrimonio (delitti contro)*, in *Digesto delle discipline penalistiche*, IX, Torino, 1995, p. 281.

[78] Relativamente a contenuti ed implicazioni della teoria personalistica costituzionalmente orientata, che include ogni unità strumentale al soddisfacimento di bisogni materiali e spirituali, si rinvia a MOCCIA, *Tutela penale del patrimonio e principi costituzionali*, Padova, 1988, 62 ss.; F. MANTOVANI, *voce Patrimonio (reato contro il)*, in *Enc. Giur.*, XXII, 1990, p. 2 ss.; CARMONA, *Tutela penale del patrimonio individuale e collettivo*, *cit.*, 66 ss..

[79] In questi termini MAZZANTINI, *La tutela del patrimonio alla prova della smaterializzazione dei rapporti socio-economici. La centralità dei delitti di frode nel sistema penale "vivente"*, *cit.*, p. 85, per cui "*nella Costituzione il patrimonio è utilità, ricchezza, entità che trova la propria naturale relazione con i fatti economici che ne rappresentano l'origine e la destinazione*".

[80] Questi scopi di tutela collettiva sono posti dagli art. 41 e 42 relativi rispettivamente all'iniziativa economica e alla proprietà. Per FIORELLA, *L'economia pubblica e privata quale oggetto dell'offesa e parametro del campo di materia, cit.*, p. 463, queste disposizioni programmatiche sarebbero "*veicoli qualificati per la tutela dell'economia pubblica e privata, comprensiva del patrimonio dei singoli*"; per CARMONA, *op. cit.*, p. 257 farebbero parte di quella che è la nostra "*costituzione economica*", la quale rifletterebbe l'ideale del capitalismo popolare, a sua volta espressione del principio della dignità umana.

[81] In questa direzione ZATTI, *La dimensione costituzionale della tutela del risparmio. Dalla tutela del risparmio alla protezione dei risparmiatori/investitori e ritorno?*, in *Forum di quaderni costituzionale rassegna*, 2010, p. 7; SCUTO, *La tutela costituzionale del risparmio negli anni della crisi economica*, in *www.federalismi.it* del 25 ottobre 2019.

Alla luce di queste considerazione una nozione di patrimonio che ne abbracci la consistenza digitale appare riferibile alla titolarità di un'utilità economicamente apprezzabile, di cui vada tutelata sia l'esclusiva disponibilità[82], sia l'intangibilità e la funzionalità[83].

Una concezione di questo tipo, quale sintesi aggiornata di una visione economica-giuridica[84], evita, da un parte, di caricare il patrimonio di una prospettiva macroeconomica, che interessa il singolo solo quale beneficiario finale del sistema di tutela collettivo; dall'altra, di valorizzare la componente personalistica senza, però, far evaporare quella connessa all'integrità patrimoniale quale oggetto di tutela in sé.

[82] MAZZANTINI, *La tutela del patrimonio alla prova della smaterializzazione dei rapporti socio-economici. La centralità dei delitti di frode nel sistema penale "vivente"*, *cit*., p. 87, il quale affianca alla disponibilità anche l'accessibilità.

[83] Con riferimento alla ricorrenza di questo aspetto alla base dell'estensione del concetto codicistico di violenza sulle cose ed in generale sull'incidenza delle TIC e della nuova dimensione del Cyberspace sul "*contenuto lesivo dei "fatti" costitutivi di reato, integranti l'offesa di beni giuridici corrispondentemente "rinnovati" rispetto a quelli tradizionali*" Cfr. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, *cit*., p. 70.

[84] Nel senso che la visione proposta guarda comunque al patrimonio quale valore di rilevanza sia economica, sia giuridico in considerazione della natura formale del relativo rapporto sui beni che lo incorporano, secondo la concezione mista maggioritaria in dottrina. Senza pretesa di esaustività si rinvia sull'analisi di questa concezione a MILITELLO, *voce Patrimonio (delitti contro)*, *cit*., p. 287, che propende per l'impossibilità di separare completamente le due ottiche, quella giuridica e quella economica, nella storia dogmatica del concetto penalistico di patrimonio; FIANDACA-MUSCO, *Diritto penale. Parte speciale*, vol. II, 7 ed., 2015, p. 25; ANTOLISEI, *Manuale di diritto penale. Parte speciale*, vol. I, 16 ed., 2016, p. 379, il quale, pur dichiarando di optare per una concezione giuridica, ricostruisce l'offesa al patrimonio come violazione di "*un obbligo di non ingerenza relativo ad un rapporto patrimoniale e, precisamente, ad un rapporto che abbia come proprio oggetto o un valore economico o di affezione*". Per una disamina più ampia del panorama dottrinale sul punto si rinvia a FORMICA, *Introduzione. I reati contro il patrimonio*, in VIGANÒ, PIERGALLINI (a cura di), *Reati contro la persona e contro il patrimonio*, *cit*., p. 382-383; in senso critico sulla funzione identificativa di queste concezioni vedi MARINI, *Delitti contro il patrimonio, cit*., p. 17-22, che propende per la "*la tendenziale convenzionalità del riferimento al patrimonio quale oggetto di tutela*".

Capitolo II

La consistenza delle criptovalute

Sommario: 1.Analisi fenomenologica, 2. *Second generation of blockchain*, 3. Le valute virtuali nella prospettiva del bene giuridico, 4. Le valute virtuali quale oggetto materiale di reato.

1. *Analisi fenomenologica*

Le valute virtuali sono una delle forme di manifestazione del binomio tecnologia e finanza[85] maggiormente dirompente rispetto alle coordinate classiche dei sistemi economici tradizionali ed in particolare monetari[86].

Espressione della "*democratizzazione dei mercati*"[87] e di quella che viene definita l'era dell'«*Internet delle Transazioni*»[88], l'evoluzione degli scambi in valute virtuali ne ha messo in luce sviluppi a carattere speculativo finanziario, che vanno oltre la funzione di meri mezzi di pagamento, in origine a loro attribuita[89]. Non si tratta semplicemente della possibilità di guadagni derivanti dalle

[85] GRECO, *Valute virtuali e valute complementari, tra sviluppo tecnologico e incertezze regolamentari*, in *Rivista di diritto Bancario*, 1/2019, p. 91.

[86]In questo senso CIAN, *La criptovaluta-alle radici dell'idea giuridica di denaro attraverso la tecnologia: spunti preliminari*, in *Banca Borsa Titoli di Credito*, 3/2019, p. 315, secondo cui "*Il primo dato che balza agli occhi, e in cui massimamente si manifesta la portata del fenomeno come esperienza di rottura rispetto agli schemi economico-giuridici tradizionali, è quello della spontaneità e della diffusività che caratterizza il momento genetico delle principali fra queste "monete": non esiste un'entità emittente e la "moneta" si genera grazie all'operatività di software installati su una pluralità di terminali e tra loro interconnessi, secondo le regole codificate ex ante nel software stesso*".

[87] DI VIZIO, *Lo statuto penale delle valute virtuali,* in www.discrimen.it, del 19 giugno 2019, p. 3, il quale discorre di ripudio dell'intermediazione di autorità centrali nelle transazioni private, di ribellione alla pervasività del controllo statuale sul sistema economico.

[88] FERRARO, *Fintech. La digitalizzazione della finanza tra Criptovalute e Blockchain*, in *IPE Working Paper*, 18/2019, p. 21.

[89] In questo senso BONAIUTI, *Schemi di pagamento e valute virtuali*, in *Moneta e Credito*, vol. 72, 288/2019, p. 405-406, per cui alla base della finanziarizzazione concorre il fatto che la proprietà dei bitcoin in circolazione è assai concentrata: "*La decisione di ottenere un indirizzo bitcoin – evidenziata in altri studi – non coincide con l'idea di utilizzarlo per finalità transattive correnti, come gli acquisti on line, e ciò spiegherebbe la non movimentazione di una parte considerevole (intorno al 50%) dei bitcoin sin qui originati (…)Se il bitcoin come mezzo di scambio avesse incontrato il favore che si attendevano i suoi ideatori, la questione degli Exchange non sarebbe stata così rilevante: si sarebbe costituito, infatti, un circuito di pagamento sempre più esteso in relazione al numero degli esercizi in cui era possibile spendere la nuova criptomoneta*".

oscillazione del tasso di conversione in moneta reale o dalla loro intrinseca volatilità[90], ma di veri e propri investimenti a rischio, a cui è associata la promessa di un rendimento finanziario[91].

Ne deriva che ai fini della qualificazione giuridica delle valute virtuali diviene centrale la comprensione della funzione sostanziale che vi si cela, la quale, conformemente alla molteplicità d'impieghi della tecnologia di base, può essere variamente conformata[92].

Nello specifico, la *blockchain*[93], diffusasi soprattutto con lo sviluppo del *bitcoin*[94], è solo una delle tecnologie basate sulla c.d. *distributed ledger technology* (DLT), la quale, a sua volta, non può essere esclusivamente assimilata alle valute virtuali[95].

Il c.d. decreto semplificazione del 2019 ha fornito una definizione normativa di di*stributed ledger technology* includendo "*tutte le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e*

---

[90] In proposito DI MARTINO, *Soluzione e prospettive sulla "natura giuridica" delle valute virtuali*, in CASSANO, DI CIOMMO, DE RITIS (a cura di), *Banche, Intermediari e Fintech, Nuovi strumenti digitali in ambito finanziario*, Giuffrè, 2021, p. 309, per cui l'andamento inflazionistico o deflazionistico è in parte causa ma anche conseguenza dell'attività d'investimento speculativo.

[91] DI MARTINO, *Soluzione e prospettive sulla "natura giuridica" delle valute virtuali*, *cit.*, p. 312, che distingue a secondo della causa del negozio, se la disponibilità finanziaria è investita per trarne profitto o per soddisfare bisogni del disponente; in questo senso anche PERNICE, *Criptovalue e bitcoin,* in FIMMANÒ, FALCONE (a cura di), *FinTech, cit.*, p. 537.

[92] Questo approccio è stato applicato dal Tar Lazio, sezione II ter, 28 gennaio 2020, n. 1077, con nota di DI GIALLUCA, GARSIA, GIUNTA, in *Diritto di internet*, 2/2020, p. 349 ss., per cui "*Il trattamento fiscale delle valute virtuali va ricondotto alle forme di tassazione già esistenti in forza della natura delle operazioni poste in essere mediante detti valori (oltre che, naturalmente, in base alla natura dei soggetti utilizzatori e delle relative attività, imprenditoriali o meno), laddove (e nella misura in cui) detto utilizzo generi materia imponibile. L'iscrizione delle valute virtuali nel quadro RW consegue a obblighi dichiarativi già esistenti, come definiti ai sensi del d.l. 28 giugno 1990 n. 167 (cd. decreto sul "monitoraggio fiscale")*". Gli autori, in particolare, mettono in luce come l'accoglimento di una nozione "funzionale" della moneta virtuale comporta che è soggetta a tassazione non la moneta virtuale come mezzo finanziario in sé, ma il suo utilizzo ai diversi fini che essa rende possibili (finanziari o di acquisto di beni e servizi, a seconda dei casi).

[93] Sulla natura e caratteristiche di questo database aperto e distribuito contenente una sequenza di dati immutabili e sulle sue applicazioni pratiche non più confinate alle cripto-valute si rinvia a VISCONTI, *La valutazione delle blockchain: internet of value, network digitali e smart transaction,* in *Il Diritto Industriale* n. 3/2019, p. 302-303.

[94] Sull'origine di *bitcoin* "*come una moneta virtuale in grado di unire le caratteristiche del trasferimento peer-to-peer di potere di acquisto, (tipico della moneta legale) garantendo la non contraffazione senza l'esistenza di una autorità di controllo (tipica della moneta merce), insieme alla facilità di utilizzo consentita dalla forma elettronica (tipica della moneta bancaria e della e-money)*" vedi BONAIUTI, *Schemi di pagamento e valute virtuali*, *cit.*, p. 401-402.

[95] SALVATORE, *Blockchain e 231,* in *(La) Responsabilità amministrativa delle società e degli enti*, 2/2020, n. 2, p. 249 ss., il quale mette in luce come la tecnologia blockchain fa parte della Industry 4.0, potendo essere oggetto delle applicazioni più svariate, anche nel settore della compliance. Sul recente successo dei *not Fungible Tokens*, nuovo filone del collezionismo, ed in generale sulla cryptoart, quale arte digitale che sfrutta per la sua commercializzazione e conservazione questa tecnologia, si rinvia rispettivamente a https://www.ilsole24ore.com/art/-la-blockchain-l-arte-digitale-diventa-unica-e-immortale-consapevolezza-un-etica-dell-intelligenza-artificiale-AE1CV8GH e https://www.repubblica.it/dossier/stazione-futuro-riccardo-luna/2021/03/11/news/l_arte_e_il_collezionismo_nell_era_della_blockchain-291717228/.

non modificabili"[96]. Ed ha collegato al suo funzionamento gli effetti giuridici della validazione temporale elettronica, di cui all'art. 41 del Regolamento UE n. 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno[97].

In particolare, il registro aperto e distribuito è costituito da una lista di nodi tra loro collegati, resi sicuri mediante l'uso della crittografia asimmetrica[98] e specificamente da un sistema a doppia chiave, pubblica e privata, con le quali i singoli nodi vengono univocamente indentificati da un *hash*, differente dall'*hash* che contrassegna l'intero registro[99].

Nel caso di *blockchain* la disposizione dei blocchi avviene a catena ed in ordine cronologico secondo un sistema di "marca temporale" che identifica in maniera certa ed immutabile l'operazione con la data e l'orario di realizzazione[100]; in questo modo il singolo *hash* non è dato solo dalle informazioni delle transazioni iscritte, ma anche da quelle relative ai blocchi precedenti[101].

Nonostante quanto sopra, queste operazioni risultano sì tracciate, ma pseudo-anonime, nel senso che non sono associate all'identità dell'ordinante e del ricevente, ma ai *transaction address* che hanno

---

[96] In questi termini l'art. 8 ter della legge 11 febbraio 2019, n. 12, di conversione con modificazioni, del decreto-legge 14 dicembre 2018, n. 135, recante disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione.

[97] FAVALORO, *Decreto Semplificazioni 2019: blockchain e smart contract diventano legge*, in *Quotidiano Giuridico* del 6 febbraio 2019, il quale evidenzia come la previsione legislativa attribuisca alla registrazione di un documento nella *blockchain* la certezza circa i suoi estremi temporali, con possibilità di opporre il tutto a terzi; nello specifico si è così assimilato l'utilizzo di tecnologie basate su registri distribuiti alla validazione temporale elettronica di cui all'art. 41 del Regolamento UE n. 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno, con la conseguenza che debbono essergli riconosciuti effetti giuridici, tra cui l'ammissibilità come prova in giudizio.

[98] ROSATO, *Profili Penali della criptovalute*, *Quaderni del Centro Ricerca Sicurezza e Terrorismo*, Pacini Giuridica, 2012, p. 22, specifica come diversamente dalla crittografia simmetrica che garantisce solo la riservatezza del messaggio, in quella asimmetrica, in assenza della chiave privata per decifrare il messaggio, il soggetto terzo che lo intercetta avrebbe conoscenza della chiave pubblica del mittente ma non potrebbe prendere visione del messaggio.

[99] KROGH, *La responsabilità del gestore di piattaforme digitali per il deposito e lo scambio di criptovalute*, nota a Tribunale di Firenze, sez. fallimentare, 21 gennaio 2019, n.18, in *Diritto di Internet*, n. 2/2019, p. 348, definisce hash "*un'operazione (Non Invertibile) che permette di mappare una stringa di testo e/o numerica di lunghezza variabile in una stringa unica ed univoca di lunghezza determinata. L'Hash identifica in modo univoco e sicuro ciascun blocco. Un hash non deve permettere di risalire al testo che lo ha generato*". Sulla funzione che la crittografia ha ai fini della prevenzione delle frodi e contraffazioni e sulla definizione dei bitcoin quali *"file criptati creati da qualsiasi computer connesso alla rete software open source"* vedi ALCINI, *Mondi paralleli, "bitcoin" e reati virtuali*, in *La Giustizia penale*, 7/2018, p. 443-444.

[100] PARODI, LOMBARDO, GHIRARDI, *Il riciclaggio e l'aggiotaggio telematico*, in PARODI, SELLAROLI (a cura di), *Diritto penale dell'informatica. Reati della rete e sulla rete*, Giuffrè, 2020, p. 464, che chiariscono come attraverso il cd. *timestamping* è possibile "*associare una data e un'ora certe e legalmente valide ad un documento informatico, rendendo tale dato opponibile a terzi*".

[101] ACCINNI, *Profili di rilevanza penale delle "criptovalute" (nella riforma della disciplina antiriciclaggio del 2017)*, in *Archivio penale* n. 1/2018, p. 3.

inviato e ricevuto i *bitcoins* e nello specifico ad un codice alfanumerico coincidente con la relativa chiave pubblica di accesso che viene comunicata dal beneficiario per ricevere il trasferimento[102].

Deve, invece, essere mantenuto il più totale riserbo sulla chiave privata, che consente di "firmare"[103] la transazione/nodo, attuando i trasferimenti in valute virtuali: la sua perdita farebbe venir meno definitivamente il controllo sulle valute virtuali.

Per questa ragione le condotte di "aggressione" a queste ultime riguardano direttamente il *wallet* in cui la chiave privata è archiviata[104]. Quest'ultimo viene definito come borsellino elettronico, ma svolge in realtà funzioni non equiparabili ad un contenitore di moneta, in quanto esse vanno dall'archiviazione della chiave privata alla sua operatività ai fini delle transazioni[105].

Rispetto a questo strumento, possono assumere ruolo importante i *wallet providers*[106], i quali possono limitarsi a fornire servizi per la custodia delle chiavi private o provvedervi essi stessi per conto del

---

[102] RINALDI, *Approcci normativi e qualificazione giuridica delle criptomonete*, in *Contratto e Impresa*, 1/2019, p. 265, per cui "*un tale mascheramento non esclude la possibilità di ricavare, attraverso un incrocio dei dati contenuti nella blockchain unitamente alle tracce lasciate sul web dal soggetto che ha concretamente disposto le operazioni, la reale identità dell'individuo cui è riconducibile la chiave pubblica e, quindi, tutte le transazioni che lo hanno riguardato*".

[103] ROSATO, *Profili Penali della criptovalute*, *cit.*, p. 23, evidenzia come questa modalità riguardi specificatamente il protocollo Bitcoin, che utilizza a garanzia della paternità e genuinità delle transazioni il sistema della firma digitale: "*Il mittente "firma" con la propria chiave privata il messaggio di cui verrà successivamente verificata la paternità attraverso la chiave pubblica del mittente*".

[104] Si rinvia per l'analisi del c.d. *Key compromise criminal smart contract*, quale tipologia di *smart contract* che è programmato per trasferire una prestabilita quantità di criptovaluta alla consegna della chiave privata, che sia stata illecitamente carpita, a MINAFRA, *Le caratteristiche delle criptovalute e il loro utilizzo a fini illeciti: profili sostanziali e processuali*, in CASSANO, DI CIOMMO, DE RITIS (a cura di), *Banche, Intermediari e Fintech*, *Nuovi strumenti digitali in ambito finanziario*, *cit.*, p. 524. L'autrice discorre anche di *criminal smart contracts* per l'acquisizione e rilevazione di informazioni segrete in cui la decriptazione di questa informazione avviene automaticamente al pagamento integrale del prezzo fissato.

[105] CAPACCIOLI, *Riflessioni sulla tassazione delle criptovalute: wallet quale deposito?*, in *L'Accertamento*, 6/2020, p. 64-65, definisce il *wallet* come "portachiave" trattandosi di un software per generare, gestire, archiviare e utilizzare chiavi pubbliche e private. L'autore, sulle base delle indicazioni degli organi di normazione tecnica, distingue tra: 1. *wallet on line*, a cui si accede mediante web browser e credenziali; 2. il *wallet desktop o mobile*, si tratta di software installabili su pc o smartphone; 3. il *wallet hardware*, che si divide in quelli, come ad es. il *paper wallet*, che consentono solo la conservazione della chiave privata in un supporto fisico, e quelli che permettono anche di effettuare transazioni, ma con la garanzia dell'archiviazione della chiave privata in un supporto esterno simile alla chiavetta usb; 4. il *brain wallet* in cui il soggetto memorizza il *seed* da cui può estrarre tutte le sue chiavi private.

[106] I *wallet providers* sono definiti, all'art. 1 comma 2, lett. ff bis del d.lgs. 231/07, come modificato dal d.lgs. n. 125/2019, di attuazione della V direttiva antiriciclaggio UE 2018/843, come "*ogni persona fisica o giuridica che fornisce, a terzi, a titolo professionale, anche on line, servizi di salvaguardia di chiavi crittografiche private per contro dei propri clienti, al fine di detenere, memorizzare e trasferire valute virtuali*". Sull'inserimento in questo modo di questi soggetti tra gli obbligati antiriciclaggio sia consentito rinviare a SICIGNANO, *Gli obblighi antiriciclaggio degli operatori in moneta virtuale: verso l'autocertificazione per gli utenti della blockchain?*, in *Diritto Penale Contemporaneo Rivista trimestrale*, 4/2020, p. 146 ss; volendo VADALÀ, *Criptovalute e cyberlaundering: novità antiriciclaggio nell'attesa del recepimento della Direttiva (UE) 2018/1673 sulla lotta al riciclaggio mediante il diritto penale*, in www.sistemapenale.it del 6 maggio 2020.

cliente[107]. In questi casi fondamentale è l'affidabilità e il livello di resilienza del *wallet provider*, essendo nella disponibilità dello *user* solo il login e la password per accedere alla piattaforma ed impartire i relativi ordini di disposizione[108].

Anche la protezione di questi dati è in realtà altrettanto importante, essendo state elaborate, analogamente ai servizi *homebanking*, tecniche di *phishing*[109] relative alle valute virtuali che passano dall'apprensione di queste informazioni fino alla creazione di false *app* di portafogli elettronici mediante le quali attuare le c.d. *wallet address scams*[110] o finte *ICO (Initial Coin Offering)*[111], simili apparentemente a quelle di siti realmente esistenti[112].

A complicare il tutto, rendendo le valute virtuali particolarmente appetibili per finalità di riciclaggio[113], è la possibilità che l'*user* decida di ricorrere a servizi di *mixing*[114], mediante i quali non

---

[107] CAPACCIOLI, *Riflessioni sulla tassazione delle criptovalute: wallet quale deposito?*, *cit.*, p. 66 che evidenzia come nel caso di *custodian wallet provider* la custodia può essere *proper*, alla stregua di un ordinario servizio fiduciario, o *full,* in cui praticamente il provider gestisce nell'interesse di altri chiavi private che sono sue.

[108] Volendo in proposito VADALÀ, *La disciplina sugli usi e abusi delle valute virtuali*, in *Diritto di Internet*, 3/ 2020, p. 402.

[109] Sulla ricostruzione di questo fenomeno e sul relativo inquadramento penalistico si rinvia a CAJANI, COSTABILE, MAZZARACO, *Phishing e furto d'identità digitale. Indagini informatiche e sicurezza bancaria,* Giuffrè, Milano, 2008; FLOR, *Phishing e profili penali dell'attività illecita di "intermediazione" del cd. Financial manager*, in *Diritto penale e processo*, 1-2012, p. 55 ss.; PIANCASTELLI, *La ricezione di somme di denaro provento di phishing: risultanze investigative e problemi applicativi in punto di qualificazione giuridica*, in *www.dirittopenalecontemporaneo.it*, 3 marzo 2015. Con specifico riferimento al phsihing connesso alle valute virtuali vedi BONCOMPAGNI, *Crimini informatici e criptovalute*, in CAPACCIOLI, *Criptoattività, criptovalute e bitcoin*, Giuffrè, 2021, p. 305-306

[110] E' quanto accaduto con l'*app Trezor Mobile Wallet,* che è stata bloccata da *Google Play*; la predetta *app,* anziché rimandare al popolare portafoglio di criptovalute *Trezor* dirottava l'utente su un'altra falsa *app* chiamata *Coin Wallet* con conseguente esecuzione di trasferimenti di moneta virtuale sui *wallet* degli hacker. Si rinvia in proposito al seguente link https://www.repubblica.it/tecnologia/sicurezza/2019/05/30/news/google_play_rimosse_false_app_di_trezor_per_criptovalute-227557851/.

[111] DI LERNIA, *Crowdfunding @ICOs: esigenze di prevenzione del rischio di commissione di reati nell'era della digital economy*, in *Diritto Penale Contemporaneo Rivista trimestrale*, fasc. 2/2019, p. 103-104, definisce le ICOs, al pari delle piattaforme di crowdfunding, come "*strumenti di "disintermediazione della raccolta di risparmio per finanziare, direttamente e senza intermediari, progetti imprenditoriali e tecnologici con ambizione di scala globale*".

[112] E' accaduto per *Lybra* la valuta virtuale di *Facebook*. La vicenda mediatica è stata trattata da diverse testate giornalistiche on line tra cui Il Sole 24 ore, a cui si rimanda al seguente indirizzo https://www.ilsole24ore.com/art/si-puo-gia-comprare-libra-occhio-prima-truffa-valuta-facebook-ACicBba. Si rinvia invece, al seguente link https://www.ilsole24ore.com/art/new-york-processa-ignatov-guru-criptomonete-fantasma-ACwKAIZ, per l'applicazione anche alle valute virtuali di meccanismi tradizionali di truffa, come lo schema Ponzi in cui si è spinti ad acquistare inesistenti valute virtuali con riconoscimento di premi ed ulteriori guadagni per chi recluti nuovi investitori, a loro volta vittime della truffa.

[113] Cfr. PICOTTI, *Profili penali del cyberlaundering: le nuove tecniche di riciclaggio*, in *Riv. Trim. dir. pen. ec.*, 3-4/2018, p. 604, per cui "*l'attrazione che offrono tali "criptovalute" nasce soprattutto dall'anonimato che garantiscono a chi le utilizza e dalla totale riservatezza che accompagna le singole operazioni con esse effettuate, oltre alla loro connaturata transnazionalità, immediatezza e flessibilità di utilizzo nel Cyberspace. Per cui esse circolano in prevalenza nel dark web, prestandosi, come anticipato, alle più disparate attività e transazioni illecite (traffici di droga, armi, medicinali, organi, prostituzione, estorsioni, investimenti speculativi di ogni genere), potendo essere accettate e scambiate in tempo reale e senza alcun vincolo o controllo in ogni parte del globo*".

[114] Si rimanda per un'analisi di questi servizi a D'AGOSTINO, *Operazioni di emissione, cambio e trasferimento di criptovaluta: considerazioni sui profili di esercizio (abusivo) di attività finanziaria a seguito dell'emanazione del D. Lgs.*

sarà possibile individuare e associare per le singole operazioni i conti di entrata e quelli di uscita. Quanto sopra vale ad esempio per i *bitcoins*[115], mentre per altre valute dette *Altcoins*, come Monero, il protocollo di funzionamento riduce ulteriormente la pubblicità delle transazioni ed include un sistema di *mixing* automatico[116]. Tra gli escamotage che impediscono l'identificazione di chi opera in valute virtuali vi è, anche, l'uso dei *Virtual Private Network* e del browser Tor[117].

Aspetto dirimente di questa tecnologia è la decentralizzazione, nel senso che la validazione delle operazioni identificate nei blocchi è diffusa o parzialmente tale: a secondo se *permissionless* o *permissioned/ semipermissioned* questa operazione può essere compiuta indifferentemente da ciascun partecipante o solo da alcuni, ma in ogni caso senza l'intervento di un intermediario o di un'autorità centrale[118].

Tale attività, c.d. *mining*, viene eseguita mediante quelli che sono definiti meccanismi del consenso: quello più noto è il *Proof-of Work*[119] consistente nella decriptazione, da parte di coloro che posseggono appositi software e hardware, attraverso complessi calcoli matematici, della chiave criptata del *wallet* da cui partirà il trasferimento. Il *miner* che riesce ad operare per primo la predetta decriptazione riceve in riconoscimento un dato ammontare del valore negoziato sulla piattaforma[120].

90/2017, in *Rivista di diritto Bancario*, fasc. 1/2018, p. 11-12, che ne definisce in questi termini il funzionamento: "*un utente deposita un determinato ammontare di criptovaluta su uno o più conti di ingresso, per poi riprendersi il denaro virtuale su conti di uscita preesistenti o appositamente creati. Il mixer farà in modo che non sia possibile associare direttamente l'ammontare di denaro depositato all'ammontare ritirato alla fine, e tratterà – quale corrispettivo della propria intermediazione – una percentuale sul valore della transazione*".

[115] Si rinvia a SICIGNANO, *Bitcoin e riciclaggio*, Giappichelli, Torino, 2019, p. 23 ss., per l'analisi di come è nata questa moneta virtuale, su come funziona e quali caratteristiche peculiari ha.

[116] ACCINNI, *op. cit.*, p. 8.

[117] MINAFRA, *Le caratteristiche delle criptovalute e il loro utilizzo a fini illeciti: profili sostanziali e processuali*, *cit.*, p. 519. Sull'utilizzo da parte della criminalità organizzata del sistema TOR sia per operare anonimamente in rete, sia per le cripto-valute vedi ANSELMI, *Onion routing, cripto-valute e crimine organizzato*, *Quaderni del Centro Ricerca Sicurezza e Terrorismo*, Pacini Giuridica, 2019, p. 24 ss..

[118] RINALDI, *Approcci normativi e qualificazione giuridica delle criptomonete, cit.*, p. 265, discorre di *"trustless trust vale a dire un meccanismo di affidamento collettivo che per sostenersi ed operare non ha bisogno del supporto di organi gerarchicamente sovraordinati rispetto ai suoi utilizzatori: gli eventuali contrasti non vengono risolti attraverso l'intervento di un'autorità sovraordinata, ma automaticamente, nell'approccio strutturalmente decentralizzato del consenso distribuito. Questi stessi attributi rendono bitcoin difficile da censurare o manomettere, in quanto non vi è un punto centrale di controllo che può essere bloccato oppure condizionato. Il sistema, tuttavia, resta astrattamente fallibile"*.

[119] DAVOLA, *Distributed ledger technology, blockchain e mercati finanziari*, in CASSANO, DI CIOMMO, DE RITIS (a cura di), *Banche, Intermediari e Fintech*, *Nuovi strumenti digitali in ambito finanziario*, *cit.*, p. 68, il quale mette in evidenzia come si tratta di uno dei meccanismi applicabili, i quali sono tutti accumunati dal medesimo obiettivo "*impedire che soggetti diversi dalle parti di una transazione abbiano l'accesso alla medesima e contestualmente, sottrarre l'onere di controllo circa la legittimità delle operazioni ad un'autorità centrale, delegandolo alla comunità dei partecipanti della piattaforma*". ROSATO, *Profili Penali della criptovalute*, *cit.*, p. 29, individua tra gli altri meccanismi applicabili a minor impatto energetico, il "*proof of stake*", in cui "*il nodo che va ad aggiungere un blocco viene scelto in base alla quantità di criptovaluta che possiede, considerando anche (a seconda dei casi) da quanto tempo le detiene. L'ammontare posseduto viene "scommesso" (put at stake), e nel caso di azioni fraudolenti, il miner perderà ciò che ha messo "at stake'', come se fosse un deposito cauzionale. In questo modo, esso sarà incentivato ad agire onestamente per non perdere la somma depositata, che sarà maggiore dei ricavi dell'agire disonestamente*".

[120] D'AGOSTINO, *op. cit.*, p. 10, che mette in luce come la creazione, mediante conferimento, di valuta virtuale di nuovo conio è, da un lato, la contropartita della volontaria messa a disposizione di software ed energia elettrica

Il meccanismo delineato rende, così, possibile scambi *peer- to- peer* senza connessione ad un server centrale: sulla base della condivisione dei dati, che verranno registrati nel *database* comune, saranno possibili non solo i trasferimenti in sé, ma anche la certificazione delle transazioni, nonché l'emissione di nuova valuta.

2. *Second generation of blockchain.*

L'evoluzione e diffusione della tecnologia DLT porta ad individuare una "*first generation of blockchain*", relativa all'intermediazione e allo scambio di valute virtuali quali mezzo di pagamento, ed una seconda fase, che si affianca alla prima, senza sostituirla, "*infrastrutturalmente idonea a perseguire ulteriori e specifiche finalità negoziali attraverso software distribuiti altresì noti come smart contracts*"[121].

Le valute virtuali espressione della prima fase fungono essenzialmente da mezzo di scambio, ancorché su base consensuale[122]: "*nella misura in cui esse vengono accettate quale mezzo di pagamento di beni e servizi e veicolano pertanto permanentemente un proprio potere d'acquisto, assumono nel contesto della circolazione dei beni medesimi il ruolo tipico della moneta, consentendo al loro titolare di negoziarle in cambio dell'aspettativa al conseguimento futuro di altri beni entro la comunità che convenzionalmente la riconosce*"[123].

Questo ruolo è fortemente condizionato dal livello d'interazione con la moneta tradizionale. In proposito le valute virtuali si distinguono in "chiuse", che non sono né acquistabili, né convertibili in moneta reale e sono utilizzabili esclusivamente nel mondo virtuale, ed "aperte", acquistabili e convertibili in moneta legale, a loro volta suddivise in aperte bidirezionali, connotate da una convertibilità piena, ed aperte unidirezionali, acquistabili in moneta reale ma non convertibili nella stessa[124]. In considerazione delle caratteristiche sopra delineate, nella diffusione delle valute virtuali un peso dirimente hanno avuto le piattaforme di cambio, i c.d. *exchangers*, che sono stati, non a caso, i primi destinatari d'interventi normativi, quale l'estensione della disciplina antiriciclaggio, al fine

finalizzata ad aumentare la potenza di calcolo dell'infrastruttura tecnologica, dall'altro lo strumento per prevenire fenomeni di *double spending*.

[121] GITTI, *Emissione e circolazione di criptoattività tra tipicità e atipicità nei nuovi mercati finanziari*, in *Banca borsa e titoli di credito*, 2020, fasc. 1, p. 13.

[122] GRECO, *Valute virtuali e valute complementari, tra sviluppo tecnologico e incertezze regolamentari*, *op. cit.*, p. 18 che mette in rilievo come la "*valuta virtuale non abbia efficacia solutoria legale, ma solo su base convenzionale, cioè laddove il beneficiario accetti la predetta valuta come mezzo di estinzione dell'obbligazione pecuniaria*".

[123] Così CIAN, *La criptovaluta-alle radici dell'idea giuridica di denaro attraverso la tecnologia: spunti preliminari*, *cit.*, p. 325.

[124] Sulle categorie indicate si rinvia a BOCCHINI, *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in *Diritto dell'Informazione e dell'Informatica*, 1/2017, p. 27.

proprio di "*censire gli estremi, ossia i momenti di contatto tra il circuito della moneta avente corso forzoso e quello della moneta virtuale*"[125].

Sono, invece, espressione della seconda fase le piattaforme come Ethereum, che è "*una blockchain pubblica, dotata di una propria criptovaluta (ether) e di una piattaforma open-source attraverso la quale è possibile sviluppare, elaborare e gestire smart contract in modalità peer to peer*"[126].

Sempre il decreto semplificazione del 2019 ha definito *smart concract* "*un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse*"; nonostante la terminologia normativa, non si tratta di un contratto in senso tecnico giuridico, ma di un'operazione economica che si svolge tra più parti sulla base di un congegno automatizzato che la rende possibile[127].

Al pari di quanto esposto per la *blockchain*, questo strumento non esaurisce la sua rilevanza con riferimento alle valute virtuali[128], ma costituisce un'applicazione che ne "arricchisce" i contenuti attraverso la configurazione di *asset* digitali, cd. token, veicolati attraverso ICO[129].

---

[125] Così URBANI, *La disciplina antiriciclaggio alla prova del processo di digitalizzazione dei pagamenti*, in *Rivista di diritto bancario*, 5/2018, p. 13. Si rappresenta che con il d.lgs. n. 90/2017 gli *exchangers* erano stati inseriti nella categoria degli operatori non finanziari dei soggetti obbligati all'osservanza e applicazione delle disposizioni del decreto antiriciclaggio (art. 3, comma 5, lett. i, d.lgs.n. 231/2007) "*limitatamente allo svolgimento dell'attività di conversione di valute virtuali da ovvero in valute aventi corso forzoso*"; con il d.lgs. 125/2019 è venuta meno questa limitazione, includendosi anche "*i servizi di emissione, offerta, trasferimento e compensazione e ogni altro servizio funzionale all'acquisizione, alla negoziazione o all'intermediazione nello scambio delle medesime valute*". In questo modo si è esteso il monitoraggio delle operazioni in valute virtuali in modo da ricomprendere "*gli emittenti di "token" nell'ambito di initial coin offering e tutti gli altri soggetti che, a titolo professionale, erogano servizi nel mondo delle valute virtuali*". Così testualmente, CONSO, FERRETTI, AMENDOLA, *Antiriciclaggio e valute virtuali*, in *Rivista della Guardia di Finanza*, 3/2020, p. 795 ss., i quali in generale si sono espressi favorevolmente a questo approccio onnicomprensivo perché evita il rischio di futuri vuoti applicativi, data l'evoluzione incessante e dai confini incerti del mercato delle criptovalute.

[126] In questi termini PIRANI, *Gli strumenti della finanza disintermediata: Initial Coin Offering e blockchain, in Analisi Giuridica dell'Economia*, 1/2019, p. 331.

[127] Sulla portata della previsione normativa e la valenza in generale dello *smart contract* si rinvia a SARZANA DI S.IPPOLITO, *Blockchain e smart contract nel nuovo Decreto Semplificazioni,* in *Diritto di internet*, 1/2019, p. 17 ss.; REMOTTI, *Blockchain smart contract. Un primo inquadramento, in Osservatorio del diritto civile e commerciale*, 1/2020, p. 189 ss.; RAMPONE, "*Smart contract*": *né* "*smart*", *né* "*contract*", in *Rivista di diritto privato*, 2/2020, p. 241 ss..

[128] Sull'utilizzo di questo strumento nell'ambito del commercio *business to consumer*, nonché nell'ambito dei rapporti *business to business* e sull'inclusione al suo interno anche di veri e propri contratti perfezionati ed eseguiti da sistemi automatizzato, quanto di applicazioni, come quelle diffuse nel mercato assicurativo, che forniscono informazioni ad una piattaforma tecnologica sulla base delle pattuizioni negoziali definite con modalità tradizionali vedi DI CIOMMO, *La conclusione e l'esecuzione automatizzata dei contratti (smart contract),* in CASSANO, DI CIOMMO, DE RITIS (a cura di), *Banche, Intermediari e Fintech, Nuovi strumenti digitali in ambito finanziari, cit.*, p. 85-89.

[129] Si rinvia sul punto alla nota 111.

Con tale termine si identifica un meccanismo di raccolta fondi, simile all'*Initial Public Offering* (IPO)[130] o al *crowdfunding*[131], necessari a finanziare un progetto imprenditoriale, mediante l'emissione di "gettoni digitali"[132], in luogo di strumenti finanziari tradizionali.

I token, acquistabili sia mediante moneta legale sia mediante valuta virtuale, attribuiscono al detentore, in forza del meccanismo automatizzato alla base degli *smart contract*, rendimenti e/o diritti relativi al progetto finanziato[133].

[130] In questo senso GITTI, *Emissione e circolazione di criptoattività tra tipicità e atipicità nei nuovi mercati finanziari, cit.*, p. 15, per cui le ICOs rimangono connotate da alcune specificità rispetto alle IPOs e specificatamente "*l'utilizzo della tecnologia blockchain permette di disintermediare le infrastrutture tipiche dei mercati dei capitali; il pagamento dei token attraverso valute virtuali muta la veste dello strumento generalmente utilizzato per il regolamento dei flussi finanziari, cioè la moneta; l'utilizzo del world wide web consente di superare l'elemento della territorialità nella promozione e nella raccolta dei capitali e la pubblicazione del c.d. white paper, nel quale vengono riportate le principali caratteristiche dell'operazione e dell'oggetto dell'offerta, supera e sostituisce alcune delle necessità relative alla disciplina del prospetto*".

[131] Sulla predetta analogia GITTI, *op. cit.*, p. 18 che rappresenta come "*nel crowdfunding il processo di abbinamento tra i promotori della campagna di finanziamento e i potenziali investitori è spesso gestito dalla piattaforma e/o dagli intermediari, nell'Initial Coin Offering tale meccanismo è del tutto assente, ciascun investitore può liberamente aderire al progetto che ritiene conforme alle proprie esigenze d'investimento, per l'appunto senza alcuna intermediazione. Il processo di sviluppo tipico di una Initial Coin Offering è, molto brevemente, il seguente: anzitutto, i promotori redigono un white paper, cioè un documento che descriva il programma di investimento, le caratteristiche del protocollo e la sua implementazione; in secondo luogo, i medesimi soggetti avviano una pre-ICO, vale a dire una prevendita di token limitata a soggetti preselezionati, tipicamente investitori istituzionali o soggetti coinvolti nella fase di progettazione; infine, viene fissata una data per l'avvio della vera e propria ICO, a partire dalla quale il pubblico potrà partecipare al progetto*".

[132] KROGH, *La responsabilità del gestore di piattaforme digitali per il deposito e lo scambio di criptovalute*, *cit.*, p. 345, che considera i token come valori mobiliari, incorporando "*al loro interno, a seconda dei casi, diritti amministrativi o patrimoniali o altre utilità legati a progetti imprenditoriali, con l'aggiunta che i diritti che incorporano si attivano, modificano o estinguono in modo automatico, secondo la logica degli smart-contract (definibili come un "protocollo di transazione computerizzato che esegue i termini di un contratto*".

[133] In proposito PIRANI, *Gli strumenti della finanza disintermediata: Initial Coin Offering e blockchain, cit.*, p. 337-338, il quale riprendendo la classificazione operata dalla FINMA, l'autorità di vigilanza su mercato finanziario svizzero, distingue tra: "*(i) payment tokens, utilizzati come mezzi di pagamento per l'acquisto di beni o servizi o facilitare il trasferimento di denaro o valori; (ii) utility tokens, permettono di usufruire del prodotto o servizio costruito grazie alla tecnologia blockchain; (iii) asset tokens, attribuiscono ai possessori il diritto a percepire i ricavi futuri eventualmente raggiunti dall'emittente. La tripartizione dei token in base alla loro funzione economica è una classificazione che non esclude la possibilità per l'emittente di creare un token in grado di coniugare al suo interno elementi caratterizzanti gli utility, asset o payment tokens. Tokens ibridi, come nel caso di un asset token che è utilizzato anche come payment: un qualcosa a metà tra un valore mobiliare e un mezzo di pagamento*".

In conseguenza di questa evoluzione appare più idonea a rappresentare il multiforme sistema[134] delle valute virtuali l'espressione *criptoasset*[135] o *virtual asset* secondo il Glossario FAFT-GAFI, che contempla, anche, una definizione conformemente ampia di *Virtual asset service provider.*

Secondo la predetta definizione si tratta di "*one or more of the following activities or operations for or on behalf of another natural or legal person: i. exchange between virtual assets and fiat currencies; ii. exchange between one or more forms of virtual assets; iii. transfer of virtual assets; iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and v. Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset*"[136].

Un aspetto centrale dell'evoluzione segnalata è, infatti, il passaggio dalla disintermediazione ad un sistema di scambio di fatto simile a quello del mercato dei capitali, connotato dall'emersione di nuovi operatori professionali.

L'attività di questi operatori non è più limitata, come nel caso dei *wallet provider*, alla sola messa a disposizione del portafoglio elettronico necessario per la detenzione e movimentazione delle valute; o ancora, per le piattaforme cd. di *exchangers,* alla vendita, ad un tasso di cambio, di valuta virtuale in cambio di moneta reale: si tratta piuttosto di "*imprese che svolgono attività di consulenza nel*

---

[134] In termini analoghi CAPACCIOLI, *Aspetti operativi e ricadute giuridiche delle cripto-attività,* in *Diritto di Internet*, n. 3/2019, p. 594, che individua come connotati che identificano questo sistema: "1. *assenza di una categoria concettuale comune che permetta la comprensione, dato che in molti schemi la transazione e l'oggetto della transazione stessa sono confusi;* 2. *polimorfismo, dato che questa innovazione assume aspetti, comportamenti, forme diverse a seconda delle circostanze, dal punto di osservazione e dal soggetto che osserva;* 3. *ambiguità, per la natura ibrida che afferisce a più concetti congiuntamente;* 4. *virtualità, dato che non esiste, è una mera iscrizione in un registro virtuale e qualunque trasferimento non comporta un passaggio fisico o giuridico, cambia esclusivamente colui che è in grado di disporne;* 5. *ubiquità, dato è presente in tutti i luoghi ed in nessun luogo allo stesso tempo, con lo sradicamento di qualsivoglia necessario collegamento territoriale, non essendoci neanche la necessità di supporti fisici;* 6. *autonomia, visto che il registro è distribuito e segue regole di iscrizione basate su un algoritmo condiviso, vale a dire con la possibilità per il sistema di svolgere le proprie funzioni senza ingerenze o condizionamenti da parte di terzi*".

[135] Per GIUDICI, *Insolvenza di un "custodial marketplace" di valute virtuali e tutela dei clienti*, in *Le Società*, 5/2020, p. 588, tale termine identifica "*sia le valute digitali, sia gli strumenti finanziari "tokenizzati", sia tutta quella congerie di altri token che offrono un qualche tipo di funzione ("utility") e che sono negoziabili su un mercato secondario*".

[136] In questo senso il FATF/GAFI che ha modificato lo standard n. 15 delle Raccomandazioni e relativo glossario, indicando le seguenti definizioni: "*A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.*". Sulla portata e contenuto di queste definizioni ed in generale per l'analisi dell'approccio adottato sul tema vedi il report FATF, *Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins*, giugno 2020 e i report *Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service*, di giugno 2019 e *Money laundering risks from "stablecoins" and other emerging assets*, ottobre 2019, tutti consultabili all'indirizzo http://www.fatf-gafi.org/. Nella medesima direzione anche CONSOB, l'Autorità italiana per la vigilanza dei mercati finanziari, con il rapporto "*Le offerte iniziali e gli scambi di cripto-attività*", 2 gennaio 2020, in *www.consob.it*, p. 6-7, con cui, al fine d'individuare le basi per una futura regolamentazione per le offerte inziali e gli scambi di cripto-attività, ha definito queste ultime come "*diverse dagli strumenti finanziari di cui all'art. 1 comma 2 TUF e da prodotti di investimento di cui al comma 1, lettere w-bis.1, w-bis.2 e w-bis.3, consistenti nella rappresentazione digitale di diritti connessi a investimenti in progetti imprenditoriali, emesse, conservate e trasferite mediante tecnologie basate su registri distribuiti, nonché negoziate o destinate a essere negoziate in uno o più sistemi di scambi*".

marketing, imprese che operano da "ICO aggregators" e svolgono funzioni di rating, imprese che svolgono attività analoga a quella delle imprese-mercato, gestendo piattaforme di negoziazione, vi sono organismi di investimento collettivo che investono in Bitcoin e altri beni digitali, fondi di venture capital specializzati in startup del mondo blockchain, imprese che offrono servizi di deposito in favore degli investitori, siano essi privati o istituzionali"[137].

3. Le valute virtuali nella prospettiva del bene giuridico.

Ricostruito il variegato scenario dei *virtual asset*, i rischi penali connessi ad un loro impiego appaiono differenti e vanno apprezzati sulla base degli specifici interessi che vengono in rilievo, dato il livello di complessità raggiunto[138].

Trattandosi di attività e servizi "*a doppio uso*"[139], considerare solo i rischi connessi ad una loro funzionalizzazione illecita è riduttivo, oltre che fortemente contrario alle tendenze evolutive dell'economia digitale. L'intervento del diritto penale rispetto a questi strumenti va prima di tutto considerato in termini protezionistici, a tutela di chi sceglie legittimamente di avvalersene per soddisfare esigenze lecite o per operare investimenti.

Sotto questo profilo, le valute virtuali correttamente impiegate sono considerabili, indipendentemente dalla connotazione "monetaria" o finanziaria, come espressione di interessi meritevoli di protezione giuridica riconducibili al bene giuridico[140] patrimonio, non potendosi dubitare, da un lato, della loro idoneità a porsi come manifestazione di ricchezza[141], dall'altro, della derivazione dalla loro perdita di un danno economico[142].

---

[137] Testualmente GIUDICI, *Insolvenza di un "custodial marketplace" di valute virtuali e tutela dei clienti*, *cit.*, p. 589 che discorre in proposito di "*altri intermediari*".

[138] In questo senso PARODI, LOMBARDO, GHIRARDI, *Il riciclaggio e l'aggiotaggio telematico*, *cit.*, per cui "*l'interprete deve, specie, in chiave penale, conoscere l'uso e le modalità di circolazione delle criptovalute, piuttosto che inquadrarle in specifici istituti. Il diritto penale prescinde in molti casi dal dato giuridico formale, privilegiando in funzione della tutela di specifici interessi le condotte nelle loro manifestazioni "sociologiche". E' quanto verosimilmente accade nel caso di specie*".

[139] PICOTTI, *Profili penali del cyberlaundering: le nuove tecniche di riciclaggio, cit.*, p. 605 che rappresenta come non si tratti di attività intrinsecamente ed originariamente illegali, ma che possono e sono utilizzate per scopi illeciti. Con specifico riferimento alla rilevanza penale e alle tecniche d'incriminazione adottata con riferimento al *dual-use software*, a quei programmi informatici che possono essere utilizzati allo stesso tempo per finalità lecite o illecite Cfr. SALVADORI, *Criminalità informatica e tecniche di anticipazione della tutela penale. L'incriminazione dei "dual-use software"*, in *Riv.it. di dir. e proc. pen.*, n. 2/2017, p. 747 ss..

[140] Per un accenno sulla vastità del dibattito dottrinale che ha interessato la categoria bene giuridico vedi la nota 65.

[141] Il termine ricchezza viene qui impiegato quale utilità di pertinenza individuale. Sull'origine dell'uso di questo termine nel diritto penale e sulle forme di tutela accordate vedi nota 39.

[142] Sulla funzione garantista che il danno svolge rispetto alla categoria dei reati patrimoniali, ancorandola ad un diritto penale a base oggettivistica, vedi F. MANTOVANI, *Diritto penale, parte speciale*, Vo. II, 7 ed, 2018, p. 37-38, il quale però ammette in termini di offesa patrimoniale anche il danno morale-affettivo. Per un

Nonostante la tutela del patrimonio sia concepita come il nucleo classico del diritto penale[143], la definizione del suo oggetto non è univoca. Nella prospettiva d'indagine prescelta appare calzante una concezione aggiornata di quella economica-giuridica, inclusiva della dimensione, anche, digitale della ricchezza, che mette in secondo piano l'aspetto della corporalità, con effetti sia sul potere di controllo, sia sulla tutela della sua integrità[144]. Rispetto a questo potere di controllo, ne sarà parte integrante e costituiva anche il momento dello scambio-trasferimento o, più genericamente, dello sfruttamento economico.

Valorizzano la dimensione assiologica di questa fase le tesi dottrinali che concepiscono il patrimonio essenzialmente come espressione di una sfera di poteri. Il riferimento corre, in particolare, a quella dottrina autorevole che identifica il patrimonio ora con la "*potenzialità economica del soggetto che si basa sul potere di signoria su beni e rapporti, ai quali la società riconosce valore economico di scambio ed esige un campo d'azione garantito dal rispetto delle regole in un quadro di legalità*"[145], ora con la "*libertà personale di instaurare ed eseguire un rapporto intersoggettivo ed a-tensionale avente ad oggetto lo scambio di valori*"[146].

Secondo questa ultima tesi l'offesa penalmente rilevante sarebbe da identificare nel pregiudizio al diritto di scambiare valori. Una prospettiva di questo tipo, spostando l'asse assiologico sull'utilità ricavabile in forza dello scambio, si adatta particolarmente alla consistenza smaterializzata delle valute virtuali: esse permettono di "*accumulare ed esportare capitali del tutto "virtuali" – il cui valore cioè non solo è espresso in formato esclusivamente digitale, ma ha fondamento soltanto convenzionale – che comunque consentono di effettuare transazioni ed acquisti, contrarre debiti ed ottenere crediti, produrre profitti finanziari e speculativi anche enormi: il tutto senza ricorrere a movimentazioni di denaro, monete o valute ufficiali, ne´ apertura od utilizzo di conti corrente bancari, ovvero appoggio ad essi, ne´ trasferimenti di comuni fondi finanziari o formali finanziamenti od anticipazioni, depositi, prelievi o mutui di tipo tradizionale, ne´ tantomeno necessità di utilizzo di carte di credito o di debito, smartcard o altri "documenti" equivalenti emessi da istituti di credito o finanziari ed intestati a soggetti determinati*"[147].

Ferma la rilevanza che il diritto a scambiare può avere in rapporto alla ricostruzione del bene giuridico patrimonio, ne appare, comunque, preferibile un'accezione più ampia incentrata sulla titolarità in generale di un'utilità suscettibile di sfruttamento economico, di cui si abbia la disponibilità lecita.

---

considerazione del danno quale requisito implicito di tutti i delitti contro il patrimonio vedi ANTOLISEI, *Manuale di diritto penale, parte speciale*, *cit*., p. 387.

[143] Così FORMICA, *Introduzione.I reati contro il patrimonio, cit*., p. 377, discorre del patrimonio come "*nucleo "tradizionale" del diritto penale*" perché la sua tutela è essenziale una società organizzata.

[144] Si rinvia in proposito al terzo paragrafo del I capitolo.

[145] Così MOCCIA, *Impiego di capitali illeciti e riciclaggio: la risposta del sistema penale italiano*, *cit*., p. 740.

[146] In questi termini FALCINELLI, *L'atto dispositivo nei delitti contro il patrimonio. Sezioni e intersezioni del sistema penale, cit*., p. 11.

[147] PICOTTI, *Profili penali del cyberlaundering: le nuove tecniche di riciclaggio, cit.*, p. 600.

Questa "disponibilità", in assenza di un sostrato materiale identificativo del diritto o della relazione di fatto sulla cosa, è riferibile ad un concetto di "appartenenza".

La dottrina penalistica ha in genere identificato l'appartenenza come quel vincolo giuridico derivante dall'insistenza di un qualsiasi diritto, non solo di proprietà, sulla cosa[148]. Rispetto ad una nozione di questo tipo, ad avviso di chi scrive, appare preferibile, in un dimensione sociale ed economica dematerializzata, una ricostruzione che la identifichi nella titolarità di un triplice potere di controllo, d'impiego e di godimento-accessibilità esclusiva.

In questo modo l'appartenenza risulta concetto inclusivo, ma al tempo stesso ulteriore rispetto a quei differenti gradi di disponibilità riferibili ad una nozione penalistica di possesso[149], la quale non è adatta ad entità digitali.

Proprio con riferimento a queste entità l'appartenenza va colto principalmente nell'autonomia dell'esercizio di quella triade di poteri che la identifica e specificatamente nella loro opponibilità "informatica" ai terzi, quale esclusività della spettanza al titolare di ammettere o escludere forme sia di condivisione della res dematerializzata, che ne riducano le potenzialità di sfruttamento economico, sia d'intervento altrui che ne possa compromettere la funzionalità.

Questi profili di tutela penale emergono nella configurazione dei reati informatici contro il patrimonio che sono previsti al titolo XIII del libro II del codice penale, come la frode informatica o le ipotesi di danneggiamento aventi ad oggetto dati e sistemi informatici[150].

Pur essendo riferiti, in virtù della collocazione sistematica, alla medesima unità assiologica dei tradizionali reati contro il patrimonio[151], sembrano proiettati verso la tutela della "*corretta e fedele*

---

[148] Cfr. CHIAROTTI, voce *Appartenenza*, in *Enciclopedia del diritto*, vol. II, 1958, p. 704 ss., che, richiamando la tesi di Carnelutti del patrimonio come aggregato di cose su cui il soggetto vanta un diritto, rappresenta graficamente l'appartenenza privatistica, che è estensibile anche al diritto penale, come un insieme di cerchi dal diametro differente, di cui quello più ampio comprende i minori.

[149] Per MARINI, voce *Possesso (diritto penale)*, in *Dig. disc. pen.*, 1995, IX, 630 ss., il possesso penalmente rilevante consiste in "*una situazione di fatto che ha a proprio contenuto una cosciente relazione materiale fra la res ed il soggetto, contraddistinta da un minimo di autonomia rispetto al titolare di un potere maggiore, accompagnata nelle singole fattispecie da altre note caratterizzanti, le quali possono variare, a seconda delle ipotesi ed a seconda della posizione del possesso nell'ambito della fattispecie, dal vero e proprio potere di fatto (corrispondente al contenuto della proprietà o di altro diritto reale, caratterizzato dalla piena autonomia rispetto al dominus e contraddistinto, inoltre, in taluni casi, dagli altri requisiti che tipicizzano il possesso in materia civilistica) ad un potere attenuato esulante persino dall'ipotesi della detenzione qualificata di cui all'art. 1168, cpv., c.c.*".

[150] Per SALVADORI, *Il " microsistema " normativo concernente i danneggiamenti informatici. Un bilancio molto poco esaltante,* in *Rivista italiana di diritto e procedura penale,* n. 1/2012, p. 238-241, la tutela del patrimonio del proprietario dei dati e sistemi informatici è presente, ma solo sullo sfondo; per questa ragione l'Autore propone in prospettiva *de iure condendo* l'inserimento di un nuovo titolo del codice sotto il bene di categoria costituito dalla sicurezza informatica e comprensivo di tutti i delitti che offendono la riservatezza, l'integrità e la disponibilità di dati e sistemi informatici.

[151] Vedi sulla portata offensiva "*rinnovata*" dei "*fatti*" costitutivi di questi reati rispetto a quelli "tradizionali" Cfr. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme*, *cit.*, p. 70.

attivazione nonché esecuzione delle procedure programmate, contro il rischio di interventi non solo manipolatori in senso stretto, ma anche meramente abusivi"[152].

4. Le valute virtuali quale oggetto materiale di reato.

La tutela dei sopra indicati interessi ulteriori sembra predicabile, come si avrà modo di esporre nel prosieguo, anche alle valute virtuali, le quali sulla base della definizione oggi codificata su spinta europea dal d.lgs. 231/2007 sono definite come "*rappresentazione digitale di valore, non emessa né garantita da una banca centrale o da un'autorità pubblica, non necessariamente collegata a una valuta avente corso legale, utilizzata come mezzo di scambio per l'acquisto di beni e servizi o per finalità di investimento e trasferita, archiviata e negoziata elettronicamente*" [153].

E' bene precisare che, in conseguenza della funzione propria del sistema antiriciclaggio[154], consistente nella "blindatura" di alcuni punti nevralgici del sistema economico al fine d'impedirne la contaminazione[155], la predetta definizione guarda alle valute virtuali quale ricchezza di cui va presidiata la circolazione, senza impedire o precludere, sulla base della specificità del loro contenuto sostanziale, che può essere differente, l'operatività parallela di altri regimi[156].

---

[152] Così PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, *cit*., p. 55. Nella giurisprudenza recente è esplicita sul punto Cass. pen. Sez. II, 12.12.2019, n. 50395, consultabile alla banca dati on line *www.pluris-cedam.utetgiuridica.it*., per cui "*l'art. 640 ter c.p., invece, è stato collocato tra i delitti contro il patrimonio mediante frode, con ciò rinviando anche letteralmente alla tutela del bene giuridico costituito dal patrimonio, pur se è innegabile, dalla descrizione della condotta incriminata, che la tutela investa anche il regolare funzionamento dei sistemi informatici, oltre alla riservatezza dei dati ivi contenuti*".

[153] In questi termini art. 1 punto 2) lett. qq. del d.lgs. 231/2007. Il nostro legislatore aveva già introdotto la definizione di valuta virtuale con il d.lgs. n. 90/2017 di attuazione della IV direttiva antiriciclaggio, ma con il d.lgs. 125/2019, di attuazione della V direttiva antiriciclaggio, l'ha ampliata, includendo anche la finalità di finanziamento, oltre che di scambio, che può connotare alcune valute e alcuni loro impieghi. Per un breve commento in proposito sia consentito rinviare a VADALÀ, *Criptovalute e cyberlaundering: novità antiriciclaggio nell'attesa del recepimento della direttiva (UE) 2018/1673 sulla lotta al riciclaggio mediante il diritto penale*, *cit*.. Per una più ampia disamina del contenuto della V direttiva antiriciclaggio v. PACILLO, *Le valute virtuali alla luce della V Direttiva Antiriciclaggio*, in *Rivista trimestrale di diritto tributario*, n. 3-4/2018, n., p. 631 ss.; BIXIO, *Le valute virtuali nella V Direttiva antiriciclaggio*, in *Corriere tributario*, n. 25/2018, p. 1987 ss.; MANIERI, *Quinta direttiva europea antiriciclaggio: il decreto di recepimento 125/2019 entra in vigore*, nella sezione approfondimenti di *www.dirittobancario.it* del 5.11.2019.

[154] FOLCO-SIENA, *Il legal framework europeo di contrasto al riciclaggio transnazionale verso una svolta? Problemi attuali e prospettive di revisione organica*, in *Giurisprudenza penale web*, 2/ 2021, p. 8, per cui "*Il sistema di prevenzione, in definitiva, pur non affrancandosi da quello repressivo, ha assunto nel tempo un ruolo di sicura preminenza e autonomia, sia, a monte, quale imprescindibile ed agile complemento del diritto penale, sia, a valle, quale catalizzatore di una nuova cultura della legalità nel sistema finanziario, chiamato a produrre esso stesso gli "anticorpi" necessari*".

[155] SGUBBI, *Il reato come rischio sociale. Ricerche sulle scelte di allocazione dell'illegalità penale*, il Mulino, Bologna, 1990, p. 26. Secondo l'Autore, gli strumenti sovranazionali hanno contribuito alla creazione di un sistema di prevenzione che attraverso una serie di regole tecniche e burocratiche realizza, nel settore del credito e non solo, "*una sorta di ordine pubblico tecnologico*".

[156] In questo senso D'AGOSTINO, *Offerte di criptoattività e abusivismo finanziario. I margini di rilevanza penale dell'esercizio non autorizzato di servizi di investimento*, nota a Cass. pen. Sez. II, 25.09.2020, n. 26807, in *Diritto di Internet,* n. 1/2021, p. 150, per cui "*la disciplina dei mercati finanziari si muove dunque su un piano parallelo e*

Ai fini penali la polivalenza delle valute virtuali deve essere, infatti, valorizzata e non osteggiata per prevenire e reprimere i rischi reali che ne accompagnano gli svariati impieghi, individuando le fattispecie penali effettivamente conformi alle modalità di strumentalizzazione illecita della loro concreta dimensione sostanziale.

Nello specifico, la definizione quale "*rappresentazione digitale*" individua la consistenza delle valute virtuali quale oggetto su cui ricade l'attività delittuosa[157], impedendo l'equiparazione sia al denaro o alla moneta elettronica[158], sia alla "cosa" in termini fisici naturalistici[159].

In conseguenza di quanto esposto, le valute virtuali sono state ricondotte al "dato informatico", definito dall'art. 1 della Convenzione di Budapest come "*ogni rappresentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema informatico, incluso programmi in grado di consentire ad un sistema informatico lo svolgimento di una funzione*"[160]. Di tale natura può essere considerata, anche, la stessa chiave privata, senza la quale non è possibile conseguire la disponibilità delle valute virtuali[161].

Con riferimento ai casi in cui questa disponibilità sia conseguita illecitamente, avrebbe una mera valenza ricognitiva o casistica limitarsi ad individuare le fattispecie criminose cui ricondurla.

Che possa essere, ed esempio, incriminato ai sensi dell'art. 640 c.p. la condotta di chi, prospettando finti servizi, si faccia dare quale prezzo valute virtuali, incamerandole senza alcuna contropartita, è fuor di dubbio: la carica dirompente delle valute virtuali non comporta, di per sé, dal punto di vista

---

complementare rispetto a quella dettata dal D. Lgs. 90/2017, di modo che l'applicazione dell'una non esclude l'altra e viceversa".

157 La distinzione tra oggetto materiale ed oggetto giuridico del reato che si deve a CARRARA, *Programma del corso di diritto criminale*, Lucca, 1867, è stata approfondita da A. ROCCO, *L'oggetto del reato e della tutela giuridica penale*, 1913, p. 229, il quale riferisce il primo all'"*azione che costituisce il reato*" ed il secondo all'"*offesa (lesione o minaccia) che costituisce, il carattere giuridicamente illecito (o antigiuridico) del reato stesso*".

158 Sull'esclusione della natura formale di moneta, ma sull'assunzione di fatto di questo ruolo si rinvia a PARODI, *Riciclaggio e monete elettroniche: le nuove indicazioni del d.lgs. 125/2019*, in www.llpenalista.it del 28 novembre 2019.

159 BONCOMPAGNI, *Crimini informatici e criptovalute*, in CAPACCIOLI, *Criptoattività, criptovalute e bitcoin*, cit. p. 306.

160 In questi termini ZONILE, *La regolamentazione internazionale ed europea di contrasto all'uso di valute virtuali da parte della criminalità transnazionale*, *cit*., p. 157-158, per cui, inoltre, le transazioni in valute virtuali, per il fatto di richiedere la composizione di un complesso "*mathematical puzzle*" di matrice informatica, rientrerebbero tra le forme di "*trasmissione di dati"* previste dall'art. 1, lett. d), della medesima Convenzione. Circa i contenuti della Convenzione Cybercrime e l'analisi critica delle modifiche normative adottate in conseguenza del suo recepimento con la legge di ratifica 48/2008 Cfr. PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. pen. proc*., n. 6/2008, p. 700 ss.. Si segnala che la medesima nozione di dato informatico è contenuta anche nella direttiva 2013/40/UE del 12 agosto 2013 relativa agli attacchi contro i sistemi di informazione, che sostituisce la decisione quadro 2005/222/GAI del Consiglio. Per un'analisi della funzione che questa direttiva ha nel panorama delle fonti di contrasto alla *cyber*-criminalità cfr. FLOR, *Cyber-criminality: le fonti internazionali ed europee*, in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime*, *cit*., 98 e ss.; ID., *Cybersecurity ed il contrasto ai cyber-attacks a livello europeo: dalla CIA-Triad Protection ai più recenti sviluppi*, in *Diritto di Internet*, n. 3/2019, p. 443 ss..

161 PARODI, LOMBARDO, GHIRARDI, *Il riciclaggio e l'aggiotaggio telematico*, in PARODI, SELLAROLI (a cura di), *Diritto penale dell'informatica. Reati della rete e sulla rete*, cit., p. 476.

penale l'inapplicabilità di una fattispecie, come la truffa, che , come verrà meglio illustrato in seguito, costituisce un modo di offesa del patrimonio indifferente alla connotazione informatica dell'oggetto dell'atto dispositivo della vittima, purché produttivo di "*danno con ingiusto profitto*"[162].

La questione va indagata più a fondo, cercando di comprendere come combinare le forme di protezione del patrimonio individuale con un sistema economico digitale in incessante divenire.

La sfida odierna del diritto penale è tenere il passo incalzante del tempo, evitando, laddove possibile, che la natura informatica dell'oggetto materiale o ancora del mezzo o del modo di perpetrazione del fatto criminoso si traduca in un vuoto di tutela ingiustificato, che immunizzi chi opera digitalmente o virtualmente, avvantaggiandolo rispetto a chi operi soltanto nel mondo "reale e materiale".

Le valute virtuali possono essere un banco di prova per verificare se le tecniche d'incriminazione dei delitti contro il patrimonio, sia tradizionali che informatici, siano capaci di tenere il passo della digitalizzazione del sistema economico.

[162] Cfr. PEDRAZZI, *Inganno ed errore nei delitti contro il patrimonio*, Giuffrè, 1955 p. 40, per cui è la "*cooperazione della vittima che permette al reo di insidiare il rapporto patrimoniale nella sua fase dinamica, mettendo a partito le leggi dell'autonomia privata*"; a p. 60 l'insigne Maestro chiarisce come questa cooperazione sia implicita in quel nesso di derivazione causale necessario tra l'errore e l'atto di disposizione richiesto dall'art. 640 c.p..

Capitolo III

Gli obblighi d'incriminazione della direttiva UE/2019/713

1.Gli obblighi d'incriminazione della direttiva UE/2019/713; 2. La prospettiva valoriale delle scelte d'incriminazione sovranazionali; 3. Ricostruzioni dogmatiche del legame di connessione; 3.1 Il fine di utilizzazione fraudolenta.

1. Gli obblighi d'incriminazione della direttiva UE/2019/713.

Va certamente valorizzata, rispetto alla delineata prospettiva d'indagine, la direttiva[163] UE/2019/713 del 17 aprile 2019, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti e che sostituisce la decisione quadro 2001/413/GAI del Consiglio, nel cui ambito di applicazione rientra- in quanto "*mezzo di scambio digitale*"[164] - la valuta virtuale che sia "*accettata da persone fisiche o giuridiche come mezzo di scambio, e che può essere trasferita, memorizzata e scambiata elettronicamente*"[165].

La predetta direttiva è di particolare interesse per la presente indagine, in quanto il legislatore europeo, al duplice fine di contrastare le fonti di entrata della criminalità organizzata e di garantire il regolare sviluppo del mercato digitale[166], si pone come obiettivo di individuare delle condotte da

[163] Sulla portata e cogenza degli obblighi d'incriminazione discendenti da questo tipo di atto normativo post trattato di Lisbona vedi PICOTTI, *Limiti garantistici delle incriminazioni penali e nuove competenze europee alla luce del Trattato di Lisbona*, in GRASSO, PICOTTI, SICURELLA (a cura di), *L'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona*, Milano, 2011, p. 207 ss.; ID., *Le basi giuridiche per l'introduzione di norme penali comuni relativi ai reati oggetto della competenza della procura europea*, in GRASSO, ILLUMINATI, SICURELLA, ALLEGREZZA (a cura di), *Le sfide dell'attuazione di una procura europea. Definizione di regole comuni e loro impatto sugli ordinamenti interni*, Milano, 2013, p. 65 ss.; PAONESSA, *Gli obblighi di tutela penale La discrezionalità legislativa nella cornice dei vincoli costituzionali e comunitari,* Firenze, 2009, p. 237 ss..

[164] Ai sensi dell'art. 2 della direttiva si intende per: "*a) «strumento di pagamento diverso dai contanti» un dispositivo, oggetto o record protetto immateriale o materiale, o una loro combinazione, diverso dalla moneta a corso legale, che, da solo o unitamente a una procedura o a una serie di procedure, permette al titolare o all'utente di trasferire denaro o valore monetario, anche attraverso mezzi di scambio digitali; b) «dispositivo, oggetto o record protetto» un dispositivo, oggetto o record protetto contro le imitazioni o l'utilizzazione fraudolenta, per esempio mediante disegno, codice o firma; c) «mezzo di scambio digitale» qualsiasi moneta elettronica definita all'articolo 2, punto 2, della direttiva 2009/110/ CE del Parlamento europeo e del Consiglio (12) e la valuta virtuale*".

[165] L'art. 2, lett. d) della direttiva definisce come valuta virtuale "*una rappresentazione di valore digitale che non è emessa o garantita da una banca centrale o da un ente pubblico, non è legata necessariamente a una valuta legalmente istituita e non possiede lo status giuridico di valuta o denaro, ma è accettata da persone fisiche o giuridiche come mezzo di scambio, e che può essere trasferita, memorizzata e scambiata elettronicamente*". Si rinvia per il raffronto con la nozione parzialmente differente della disciplina antiriciclaggio alla nota 153, evidenziando come al considerando 10 è precisato che "*la definizione del termine «mezzi di scambio digitali» dovrebbe riconoscere che i portafogli elettronici per il trasferimento di valute virtuali possono presentare, ma non presentano necessariamente, le caratteristiche di uno strumento di pagamento e non dovrebbe estendere la definizione di strumento di pagamento*"

[166] Sul punto sono espliciti i considerando 1-2 e 7.

incriminare aventi ad oggetto gli strumenti di pagamento immateriali equivalenti a quelle classiche della frode, del furto e dell'illecita appropriazione indebita, tipizzate dal diritto nazionale prima dell'era digitale[167].

Questo obiettivo viene, in particolare, perseguito per giungere ad un'incriminazione in maniera uniforme nel territorio dell'Unione delle frodi e delle falsificazioni dei mezzi di pagamento diversi dai contanti.

E' centrale nella strutturazione dell'intero sistema la fattispecie di utilizzazione fraudolenta[168], di cui l'art. 3 richiede l'incriminazione laddove abbia ad oggetto uno strumento di pagamento sia rubato o altrimenti illecitamente ottenuto, sia contraffatto o falsificato. Ne deriva un obbligo di prevedere una fattispecie nazionale, che, partendo dal pregiudizio, individuale e patrimoniale[169], patito da chi abbia subito la sottrazione o l'impiego di uno strumento così illecitamente connotato, lo proietta nella dimensione collettiva degli scambi a cui sono riferibili valori da preservare, come la fiducia dei consumatori nella genuinità e affidabilità dei mezzi di pagamento diversi da contanti[170].

A loro volta le condotte da incriminare, relative alla provenienza illecita dello strumento di pagamento oggetto di utilizzazione, sono distinte in due ulteriori sottocategorie: quelle per gli strumenti di pagamento materiali e quelle per gli strumenti di pagamento immateriali.

In realtà, a distinguerle non è solo l'oggetto: come sarà, in prosieguo, illustrato, la diversità terminologica è espressione di specifiche e differenti scelte di politica criminale.

---

[167] In questi termini il considerando 15.

[168] Un analogo obbligo d'incriminazione, ma senza alcuna distinzione rispetto alle altre condotte, ora definite dalla direttiva UE/2019/713 come "*connesse*", era già previsto dalla decisione quadro 2001/413/GAI del Consiglio, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti ed identificati nelle carte di credito, nelle carte eurocheque e nelle altre carte emesse da istituti finanziari, nei travellers cheque, negli eurocheque e in generale negli assegni o cambiali.

[169] In proposito è chiarito ai considerando 31 e 32 della Direttiva UE/2019/713, che: "*Le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti possono avere gravi conseguenze economiche e di altro tipo per chi ne è vittima. Quando tali frodi comportano, ad esempio, il furto d'identità, le conseguenze sono spesso più gravi a causa del danno alla reputazione e del danno professionale, del danno al rating del credito della persona e del grave danno emotivo. Gli Stati membri dovrebbero adottare misure di aiuto, sostegno e protezione per attenuare tali conseguenze. Spesso le vittime impiegano molto tempo ad accorgersi che hanno subito una perdita economica a seguito di un reato di frode o falsificazione. Nel frattempo si potrebbe innescare una spirale di reati interconnessi che aggrava le conseguenze negative per le vittime*". Sia consentito rinviare a VADALÀ, *La disciplina sugli usi e abusi delle valute virtuali*, *cit.*, p. 404, per l'esame del contenuto dell'obbligo, fissato dall'art. 16, dell'introduzione di forme nazionali di supporto sia alla persona fisica sia a quella giuridica vittima di frodi e falsificazione.

[170] In questo senso esplicito è, con riferimento in generale agli strumenti di pagamento immateriali, il considerando 9 della Direttiva UE/2019/713; mentre il considerando 10 specificatamente per le valute virtuali incoraggia "*gli Stati membri a provvedere affinché il loro diritto nazionale preveda per le future valute virtuali emesse dalle rispettive banche centrali o altre autorità pubbliche lo stesso livello di protezione dai reati di frode di cui godono i mezzi di pagamento diversi dai contanti in generale. I portafogli elettronici che consentono il trasferimento di valute virtuali dovrebbero essere coperti dalla presente direttiva nella stessa misura degli strumenti di pagamento diversi dai contanti*".

Relativamente a queste condotte, l'art. 4, sotto la rubrica "*Reati connessi all'utilizzazione fraudolenta di strumenti di pagamento materiali diversi dai contanti*", le suddivide in quattro classi[171]: le prime due riguardano quelle ipotesi che possono essere definite di derivazione e formazione illecita dello strumento di pagamento materiale diverso dai contanti; le seconde, cronologicamente successive alle prime, riguardano il possesso e lo scambio dello strumento di pagamento materiale diverso dai contanti che sia rubato, contraffatto o falsificato.

Nella prima classe sono incluse le condotte di furto e quelle genericamente indicate di "*altra apprensione illecita*", formula ampia idonea ad abbracciare tutte quelle ipotesi di acquisizione "diretta" penalmente rilevante dello strumento di pagamento "genuino". Si riferiscono, invece, alla formazione illecita di questo strumento le condotte, di cui alla lett. b) dell'art. 4, relative alla "*contraffazione e [la] falsificazione fraudolenta*"[172].

Una ricostruzione di questo tipo è confermata dalla selezione delle condotte inserite nelle altre due categorie previste dall'art. 4, lett. c) e d), e costituite rispettivamente dal possesso e dall'atto di procurare per sé o per altri lo strumento di pagamento materiale illecitamente conseguito o falsificato.

Con riferimento, in particolare, a quest'ultima condotta, che sembra essere inclusiva di quelle ipotesi di acquisizione penalmente illecita di "seconda mano", l'espressione "compresi", che la segue, sembrerebbe avere una funzione specificativa di alcune modalità esemplificative omogenee.

In realtà, se si analizzano queste modalità, l'esito è differente: sono considerabili tali le condotte di ricezione, appropriazione e acquisto, consistendo tutte in un atto d'incameramento, mentre appiano più propriamente riferibili ad una vera e propria "commercializzazione" a largo spettro quelle di trasferimento, importazione, esportazione, vendita, trasporto e distribuzione.

La differenza segnalata, espressiva del distinto disvalore che le connota, avrebbe dovuto consigliare una collocazione separata; il legislatore europeo ha preferito, di contro, adottare una disciplina comune anche con riguardo all'elemento soggettivo, prevedendo per tutte le condotte della lett. d) dell'art. 4 la finalità della destinazione all'"*utilizzazione fraudolenta*".

---

[171] Si riporta di seguito il testo integrale dell'art. 4: "*Gli Stati membri adottano le misure necessarie affinché le seguenti condotte, se commesse intenzionalmente, siano punibili come reato: a) il furto o altra illecita appropriazione di uno strumento di pagamento materiale diverso dai contanti; b) la contraffazione o falsificazione fraudolenta di uno strumento di pagamento materiale diverso dai contanti; c) il possesso di uno strumento di pagamento materiale diverso dai contanti rubato o altrimenti ottenuto mediante illecita appropriazione, o contraffatto o falsificato a fini di utilizzazione fraudolenta; d)l'atto di procurare per sé o per altri, compresi la ricezione, l'appropriazione, l'acquisto, il trasferimento, l'importazione, l'esportazione, la vendita, il trasporto e la distribuzione, di uno strumento di pagamento materiale diverso dai contanti rubato, contraffatto o falsificato, a fini di utilizzazione fraudolenta*"

[172] A conferma di un giudizio di disvalore che prescinde dall'impiego dello strumento "alterato" può essere richiamato il considerando 12, per cui "*applicando il diritto penale principalmente agli strumenti di pagamento che impiegano forme speciali di protezione dall'imitazione o dagli abusi, si intende incoraggiare gli operatori a fornire tali forme speciali di protezione agli strumenti di pagamento che essi emettono*".

Medesima finalità è prevista anche per la condotta di possesso di cui all'art. 4 lett. c), relativamente alla quale il legislatore europeo esclude la punibilità a titolo di tentativo.

Per quanto riguarda, invece, gli obblighi d'incriminazione posti dall'art. 5 con riferimento agli strumenti di pagamento immateriali diversi dai contanti, sono ripartibili nella quattro categorie previste per gli strumenti di pagamento materiale[173], ma, ad eccezione delle condotte contemplate alla lett b)[174], con una selezione tipologica differente.

Quanto sopra emerge chiaramente per le condotte previste dalla lett. a) dell'art. 5 di "*ottenimento illecito di uno strumento di pagamento immateriale diverso dai contanti, almeno se tale ottenimento ha comportato la commissione di uno dei reati di cui agli articoli da 3 a 6 della direttiva 2013/40/UE, o appropriazione indebita*".

L'ottenimento illecito di cui si chiede l'incriminazione non ha nulla a che vedere con il furto, essendo- in virtù del rinvio operato alla direttiva 2013/40/UE, relativa agli attacchi contro i sistemi di informazione- identificabile con le condotte di accesso illecito, d'interferenza illecita sui sistemi e sui dati e d'intercettazione illecita[175].

Sembra possibile ritenere che sia la derivazione da queste condotte dello strumento di pagamento immateriale a giustificare l'obbligo d'incriminazione: il disvalore della condotta non attiene all'ottenimento in sé, ma al modo che lo ha reso possibile[176].

Per quanto riguarda, invece, l'obbligo d'incriminazione della condotta che viene denominata dal legislatore europeo come appropriazione indebita, nei considerando è definita come "*utilizzo consapevole e senza diritto, a vantaggio proprio o di altri, di uno strumento di pagamento immateriale diverso dai contanti, da parte del soggetto cui è stato assegnato*"[177]. In questo modo il fulcro dell'incriminazione

---

[173] Si riporta di seguito per maggiore chiarezza il testo integrale dell'art. 5 "*Gli Stati membri adottano le misure necessarie affinché le seguenti condotte, se commesse intenzionalmente, siano punibili come reato: a) l'ottenimento illecito di uno strumento di pagamento immateriale diverso dai contanti, almeno se tale ottenimento ha comportato la commissione di uno dei reati di cui agli articoli da 3 a 6 della direttiva 2013/40/UE, o appropriazione indebita di uno strumento di pagamento immateriale diverso dai contanti; b) la contraffazione o la falsificazione fraudolente di uno strumento di pagamento immateriale diverso dai contanti; c) la detenzione di uno strumento di pagamento immateriale diverso dai contanti ottenuto illecitamente, contraffatto o falsificato a fini di utilizzazione fraudolenta, almeno laddove l'origine illecita sia nota al momento della detenzione dello strumento; d) l'atto di procurare per sé o per altri, compresi la vendita, il trasferimento e la distribuzione, o la messa a disposizione, uno strumento di pagamento immateriale diverso dai contanti ottenuto illecitamente, contraffatto o falsificato a fini di utilizzazione fraudolenta*".

[174] La lett. b) dell'art. 5 prevede le stesse identiche condotte previste dalla lett. b) dell'art. 4.

[175] Per l'analisi dei contenuti di questa direttiva con specifico riferimento alle fattispecie di accesso abusivo ai sistemi di informazione ed intercettazione illecita, di fabbricazione di *malware* e di diffusione di password si rinvia a CONIGLIARO, *La nuova tutela penale europea dei sistemi di informazione. Una prima lettura della direttiva 2013/40/UE del Parlamento Europeo e del Consiglio*, in www.penalecontemporaneo.it, del 30 ottobre 2013; FLOR, *Cyber-criminality: le fonti internazionali ed europee*, *cit*., p. 120-122.

[176] In questo senso depone, dal punto di vista linguistico, l'utilizzo dell'espressione "*the theft*" alla lett. a) dell'art.4 per gli strumenti di pagamento materiali diversi dai contanti.

[177] Testualmente ancora il considerando 15.

attiene alla violazione dei limiti di legittimazione e di disponibilità dell'assegnatario, quale ipotesi a valenza dispositiva "infedele" compatibile con il carattere immateriale dello strumento.

Con riguardo alle categorie di condotte di cui alla lett. c) dell'art. 5, si segnala il riferimento diversamente dal possesso previsto dalla corrispondente voce dell'art. 4 alla detenzione, "*almeno laddove l'origine illecita sia nota al momento della detenzione dello strumento*".

Si tratta di condizione che arricchisce ulteriormente dal punto di vista soggettivo questa condotta: a causa dell'assenza di un marchio illecito fisicamente percepibile dello strumento di pagamento immateriale, la consapevolezza di questa illiceità funge da requisito in funzione ulteriormente esplicativa della strumentalità della sua "disponibilità" diretta all'utilizzazione fraudolenta.

Al pari della lett. d) dell'art. 4, anche la medesima voce dell'art. 5 contempla l'obbligo d'incriminare l'atto di procurarsi, per sé o per altri, uno strumento di pagamento immateriale illecitamente ottenuto, indicando, però, quale ipotesi esemplificative solo le condotte di vendita, trasferimento, distribuzione e messa a disposizione[178].

A completamento degli obblighi d'incriminazione, gli artt. 6 e 7 fanno riferimento alle condotte definite come "*frode connessa ai sistemi di informazione*" e a quelle relative a "*mezzi utilizzati per commettere i reati*". La frode è definita, in particolare, come l'atto di effettuare o indurre un trasferimento di denaro, valore monetario o di valuta virtuale al fine di conseguire un ingiusto profitto con altrui danno, "*ostacolando, senza diritto, il funzionamento di un sistema di informazione o interferendo con esso*" o "*introducendo, alterando, cancellando, trasmettendo o sopprimendo, senza diritto, dati informatici*".

L'art. 7 si riferisce, invece, alle condotte aventi ad oggetto la realizzazione e diffusione "*di un dispositivo o di uno strumento, di dati informatici o di altri mezzi principalmente progettati o specificatamente adattati al fine di commettere uno dei reati di cui all'art. 4, lett. a) e b), all'art. 5, lett. a) e b) o all'articolo 6, almeno se commessi con l'intenzione di utilizzare tali mezzi*". Questa connotazione materiale così definita è certamente da preferire rispetto all'ambigua terminologia usata, per condotte analoghe, dalla decisione quadro 2001/413/GAI, sempre relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti.

In particolare, l'art. 4 della citata decisione faceva riferimento a programmi di computer il cui scopo fosse "*la perpetrazione degli illeciti di cui all'articolo 3*"[179]. Pur potendo risultare la formulazione portata

[178] Diversamente dagli strumenti di pagamento materiali, per quelli immateriali non vengono richiamate, quale condotte specificative dell'atto di procurare per sé e per altri, le condotte di ricezione, appropriazione, acquisto, importazione, esportazione e trasporto.

[179] SALVADORI, *Criminalità informatica e tecniche di anticipazione della tutela penale. L'incriminazione dei "dual-use software", cit.*, p. 759, condivide il giudizio di ambiguità, ma considera questa formulazione, laddove riferita all'oggettiva configurazione del software e sorretta dal fine d'impiego per la commissione di reati, idonea a restringere conformemente il novero dei software penalmente rilevanti.

dalla direttiva UE/2019/713 per certi versi forse troppo restrittiva[180], va apprezzato lo sforzo, attestato anche dalla contestuale previsione dell'intenzione di impiegare questi mezzi[181], di ancorare l'anticipazione della soglia di rilevanza penale a quelle condotte che siano effettivamente strumentali[182] rispetto alle condotte di frode informatica e di ottenimento illecito degli strumenti di pagamento materiali ed immateriali.

2. La prospettiva valoriale delle scelte d'incriminazione sovranazionali.

Dall'analisi svolta deriva che lo "strumentario" delineato dalla direttiva si sviluppa essenzialmente lungo la seguente direttrice: l'incriminazione in generale, ma teleologicamente condizionata delle condotte prodromiche o strumentali all'utilizzazione fraudolenta[183], con esclusione, appositamente per gli strumenti di pagamento immateriali, di fattispecie incentrate sul momento materiale dell'acquisizione e del mantenimento della disponibilità.

Questa direttrice è conseguenza, oltre che della peculiare consistenza di questi strumenti, dei differenti obiettivi di politica criminale perseguiti dalla Direttiva UE/2019/713 rispetto alla

[180] E' critico su formulazione di tal fatta, che ricalca quella analoga impiegata per condotte simile dalla Convenzione Cybercrime, SALVADORI, *Criminalità informatica e tecniche di anticipazione della tutela penale. L'incriminazione dei "dual-use software"*, *cit.*, p. 758, per cui in questo modo "*si limita eccessivamente l'ambito dell'oggetto materiale e, di conseguenza, del precetto. Un programmatore può creare, di regola, un software per diversi scopi. Quest'ultimo sarà, però, considerato tipico e quindi illecito soltanto qualora si dimostri che la sua funzione o destinazione principale è di commettere quello specifico reato o gruppo di reati (ad es. CIA offences). Allo stesso tempo un software non potrebbe integrare l'oggetto tipico nel caso in cui mediante la sua creazione si perseguano al contempo finalità lecite ed illecite. Lo stesso dicasi nell'ipotesi in cui uno sviluppatore crei un programma per uno scopo legittimo, ma successivamente si scopra che può essere impiegato anche in modo illecito. Se gli scopi presi di mira dall'originario creatore o produttore del software sono molteplici, sarà irrilevante il fatto che il suo utilizzatore lo impieghi per una finalità delittuosa, purché quest'ultima non rappresenti la sua principale funzione*".

[181] Confermativa della ricostruzione proposta è il considerando 16 della direttiva UE/713/2019 che richiama la "*necessità di evitare una criminalizzazione di tali strumenti quando essi siano prodotti e posti in commercio per fini legittimi e pertanto, anche se utilizzabili per commettere reati, non costituiscano di per sé una minaccia*".

[182] In questi termini SALVADORI, *op. cit.*, p. 783, che specifica che "*il fine specifico di commettere un fatto costitutivo di reato ovvero lesivo concorre in definitiva a puntualizzare l'oggettivo significato preparatorio che assume la condotta-base in quanto strumentale al raggiungimento di quel risultato. Soltanto qualora sussista questa connessione teleologica con il fine tipizzato si potrà dire che la condotta-base è tipica e quindi penalmente rilevante*".

[183] L'estensione "consapevole" dell'obbligo d'incriminazione alle condotte prodromiche emerge chiaramente dal tenore letterale del considerando 13 della Direttiva UE/2019/713: "*occorre un'impostazione comune del diritto penale per quanto riguarda gli elementi costitutivi della condotta criminale che contribuiscono o preparano il terreno all'effettiva utilizzazione fraudolenta dei mezzi di pagamento diversi dai contanti. Condotte come la raccolta e il possesso di strumenti di pagamento allo scopo di commettere frodi, ad esempio mediante il phishing, lo skimming, oppure indirizzando o reindirizzando gli utenti di un servizio di pagamento verso siti web falsi, e la loro distribuzione, ad esempio vendendo su Internet informazioni relative alle carte di credito, dovrebbero essere qualificate come un reato a sé stante, indipendentemente dal requisito di un'utilizzazione fraudolenta dei mezzi di pagamento diversi dai contanti. Pertanto, tali condotte criminali dovrebbero includere anche i casi in cui il possesso, l'ottenimento o la distribuzione non portino necessariamente all'utilizzazione fraudolenta di tali strumenti di pagamento. Tuttavia, nei casi in cui la presente direttiva configura il possesso o la detenzione come reato, tale criminalizzazione non dovrebbe comprendere la semplice omissione*".

precedente decisione quadro 2001/413/GAI, sempre relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti[184].

Diversamente da questa decisione, che era inquadrabile nella strategia di contrasto al crimine organizzato e al denaro sporco[185], la Direttiva UE/2019/713, oltre a considerare altri fenomeni criminali[186], intende contrastare le frodi e falsificazioni quali fattori che minano la sicurezza e ostacolano il mercato unico digitale, generando una perdita economica diretta[187].

E' sintomatica di questo cambio di prospettiva la diversa conformazione dell'obbligo d'incriminazione, alle lett. b) degli artt. 4 e 5, delle condotte di contraffazione e falsificazione senza la previsione del "*fine dell'utilizzazione fraudolenta*"[188]: la loro realizzazione è in sé concepita dal legislatore europeo come offensiva anche laddove non relativa a mezzi di scambio "monetari".

Secondo un approccio tecnologicamente neutro, in un contesto di mercato digitale in costante evoluzione è la ricorrenza della funzione di pagamento in sé a determinare la necessità di presidiare, mediante apposite fattispecie penali, la circolazione degli strumenti che ne siano portatori.

Relativamente a queste fattispecie, che dovranno essere adottate negli ordinamenti nazionali, sembra possibile una strutturazione analoga a quelle nazionali di falso nummario, previste dagli artt. 453-455 c.p.[189], e d'indebito utilizzo e falsificazione di carte di credito e di pagamento, oggi

---

[184] Pur dichiarando al considerando 8 di perseguire una criminalizzazione generalizzata dell'"*intera serie delle attività che insieme costituiscono una minaccia della criminalità organizzata in questo campo*", la decisione quadro 2001/413/GAI prevedeva degli obblighi d'incriminazione relativi solo agli strumenti di pagamento materiali, limitandosi a contemplare anche le condotte che li riguardassero che fossero poste in essere mediante computer. L'art. 2 prevedeva, peraltro, l'incriminazione, come condotte prodromiche all'utilizzazione fraudolenta e successive alla falsificazione, solo di quelle di "*ricezione, ottenimento, trasporto, vendita o cessione ad altri o detenzione di strumento di pagamento rubato o altrimenti ottenuto mediante appropriazione indebita, oppure contraffatto o falsificato ai fini dell'utilizzazione fraudolenta*". Per un esame dei contenuti della decisione quadro qui sinteticamente accennati v. VILLONI, *Una strategia europea contro il crimine organizzato: la decisione quadro del Consiglio dell'Unione Europea relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti*, in *Giur. merito*, 1/2002, p. 270-271.

[185] In questo senso esplicito il considerando 5 della decisione quadro 2001/413/GAI. Come messo in rilievo da VILLONI, *Una strategia europea contro il crimine organizzato: la decisione quadro del Consiglio dell'Unione Europea relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti*, *cit.*, p. 269, "*Una strategia di lotta integrata al riciclaggio di denaro sporco non può, dunque, prescindere dal favorire il massimo sviluppo dei mezzi di pagamento diversi dai contanti (travellers cheques, assegni, cambiali, carte prepagate, moneta elettronica basata su software, ordini di trasferimento di denaro cartacei od elettronici, carte di credito, operazioni bancarie a distanza mediante telefono o personal computer) ed in particolar modo di quelli contenenti «una forma speciale di protezione dall'imitazione o dagli abusi». Tutelando in base al diritto penale detti strumenti ed in particolare quelli connotati da sistemi di sicurezza, l'Unione europea ha in tal modo espressamente inteso «incoraggiare gli operatori» a fornire protezione ai mezzi di pagamento che essi emettono «aggiungendo così un elemento di prevenzione allo strumento»*".

[186] Il già citato considerando 1 della Direttiva UE/2019/713 indica, come ulteriori attività criminali rese possibile attraverso le frodi e falsificazione, il terrorismo, il traffico di droga e la tratta di esseri umani.

[187] In questa direzione espliciti sono i considerando 2 e 7 della Direttiva UE/2019/713.

[188] Questo fine era invece espressamente contemplato all'art. 2, lett. b), della decisione quadro 2001/413/GAI.

[189] Rinviando l'esame di queste fattispecie al paragrafo successivo, per un migliore comprensione si riporta di seguito il testo rispettivamente dell'art. 453 c.p., rubricato *Falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate*, e dell'art. 455 c.p., rubricato *Spendita e introduzione nello Stato, senza concerto, di monete falsificate*, segnalando che all'art 458 c.p. il legislatore equipara alla moneta metallica quella

trasfuse nell'art. 493 *ter* c.p.[190], a conferma della protezione anche loro tramite di "*valori riconducibili all'ambito dell'ordine pubblico, economico e della fede pubblica*"[191].

Questi valori, e non solo, appaiono certamente riferibili anche agli obblighi d'incriminazione previsti dalla direttiva in esame, i quali, come sopra riferito, sarebbero posti a garanzia della sicurezza del mercato unico digitale.

"*Ammesso che la sicurezza possa essere collegata – caso per caso – a beni giuridici meritevoli di tutela penale*", come è stato autorevolmente messo in luce, sussiste, però, il rischio "*di precipitarla nell'alveo dei concetti strumentali e strumentalizzabili dalle forze socio-politiche preminenti in un determinato momento storico. Si trasforma così il totem sicurezza nella formula in grado di legittimare qualunque tipo di incriminazione, rispetto alla quale non si possa ravvisare un interesse più univoco e specifico*"[192].

Nel caso di specie questo rischio sembra evitabile, in considerazione della portata assiologica che può essere conferita al binomio sicurezza e mercato digitale, quale manifestazione del più ampio bene identificato nella sicurezza informatica.

---

cartacea e all'art. 454 c.p. prevede delle conseguenze sanzionatorie più lievi per l'alterazione che ne scema in qualsiasi modo il valore: "*art. 453. E' punito con la reclusione da tre a dodici anni e con la multa da euro 516 a euro 3.098: 1) chiunque contraffà monete nazionali o straniere, aventi corso legale nello Stato o fuori; 2) chiunque altera in qualsiasi modo monete genuine, col dare ad esse l'apparenza di un valore superiore; 3) chiunque, non essendo concorso nella contraffazione o nell'alterazione, ma di concerto con chi l'ha eseguita ovvero con un intermediario, introduce nel territorio dello Stato o detiene o spende o mette altrimenti in circolazione monete contraffatte o alterate; 4) chiunque, al fine di metterle in circolazione, acquista o comunque riceve, da chi le ha falsificate, ovvero da un intermediario, monete contraffatte o alterate. La stessa pena si applica a chi, legalmente autorizzato alla produzione, fabbrica indebitamente, abusando degli strumenti o dei materiali nella sua disponibilità, quantitativi di monete in eccesso rispetto alle prescrizioni*"; "*art. 455 Chiunque, fuori dei casi preveduti dai due articoli precedenti, introduce nel territorio dello Stato, acquista o detiene monete contraffatte o alterate, al fine di metterle in circolazione, ovvero le spende o le mette altrimenti in circolazione, soggiace alle pene stabilite nei detti articoli, ridotte da un terzo alla metà*".

[190] Il delitto in esame è stato inserito nel codice penale dall'art. 4 del d.lgs. n. 21/2018, in attuazione della delega contenuta all'art. 1 della l. n. 103/2017 sulla riserva "tendenziale" di codice nella materia penale, e riproduce- in totale continuità- la previsione dell'art. 12 del d.l. n. 143, che era stata poi trasferita al co. 9 dell'art. 55 del d.lgs. 231/2007, valorizzandone la funzione di limitazione dell'uso del contante. In questo senso si è espressa la giurisprudenza di legittimità, tra cui Cass. pen., Sez. IV, 30 aprile 2020, n. 13492, consultabile alla banca data on line *Pluris*. Per una migliore comprensione si riporta di seguito il testo dell'art. 493 ter c.p.: "*Chiunque al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, è punito con la reclusione da uno a cinque anni e con la multa da 310 euro a 1.550 euro. Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per altri, falsifica o altera carte di credito o di pagamento o qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, ovvero possiede, cede o acquisisce tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi. In caso di condanna o di applicazione della pena su richiesta delle parti a norma dell'articolo 444 del codice di procedura penale per il delitto di cui al primo comma è ordinata la confisca delle cose che servirono o furono destinate a commettere il reato, nonché del profitto o del prodotto, salvo che appartengano a persona estranea al reato, ovvero quando essa non è possibile, la confisca di beni, somme di denaro e altre utilità di cui il reo ha la disponibilità per un valore corrispondente a tale profitto o prodotto. Gli strumenti sequestrati ai fini della confisca di cui al secondo comma, nel corso delle operazioni di polizia giudiziaria, sono affidati dall'autorità giudiziaria agli organi di polizia che ne facciano richiesta*".

[191] Così la relazione al d.lgs. n. 21/2018 di attuazione della delega contenuta all'art. 1 della l. n. 103/2017.

[192] Testualmente RISICATO, *Diritto alla sicurezza e sicurezza dei diritti: un ossimoro invincibile?*, Giappichelli, 2019, p. 10.

Quest'ultima va intesa come esigenza di garantire la legittima e corretta operatività informatica, da cui deriva, in via conseguente ed "interferenziale", la protezione delle sfere d'interessi "intercettati" dalle sue strutture e dai suoi strumenti.

In questi termini confermativa appare la natura "valoriale" del rinvio operato dalla direttiva UE/2019/713 alla direttiva 2013/40/UE, per la definizione delle condotte, relative agli strumenti di pagamento immateriali, da incriminare come equivalenti, in ambito digitale, delle forme "analogiche tradizionali" di aggressione patrimoniale: le scelte di tipizzazione delle condotte in esame sono, cioè, "giustificate" dal legislatore europeo al fine d'"*integrare e rafforzare la direttiva 2013/40/UE del Parlamento europeo e del Consiglio*"[193]. Questo legame di "dipendenza" è confermato, come è stato autorevolmente rappresentato, anche dall'ulteriore richiamo espresso alla Direttiva 2016/1148/UE, "*in quanto le attività criminali aventi ad oggetto gli strumenti di pagamento elettronici e virtuali possono essere all'origine di incidenti che dovrebbero essere segnalati alle autorità nazionali competenti*"[194].

Proprio in considerazione della loro natura, la circolazione e la conservazione degli strumenti di pagamento immateriale vanno presidiate penalmente quale espressione di quelle esigenze protezionistiche riferibili direttamente alle procedure e ai meccanismi informatici, che connotano il mercato digitale e che laddove non garantite ne comprometterebbero la stessa esistenza.

3. *Ricostruzioni dogmatiche del legame di connessione.*

Definito il sostrato assiologico di riferimento, una più completa comprensione del giudizio di disvalore espresso dagli obblighi d'incriminazione passa dalla definizione della portata dogmatica del legame di connessione sulla base del quale il legislatore ha strutturato i rapporti tra l'utilizzazione "fraudolenta" e le condotte prodromiche.

Preliminare rispetto a questa verifica è la comprensione del carattere di fraudolenza che connota l'utilizzazione punibile, sembrando conferirgli una carica propria rispetto a quello afferente alla formazione e derivazione illecita del suo oggetto.

Conferme in questo senso sembrano derivare dal raffronto con le disposizioni degli artt. 453-455 c.p.[195], che si riferiscono alla "*spendita o messa in circolazione*" della moneta contraffatta o alterata, senza alcuna ulteriore connotazione[196].

---

[193] In questi termini il considerando 15 della direttiva UE/2019/713.

[194] Così FLOR, *Cybersecurity ed il contrasto ai cyber-attacks a livello europeo: dalla CIA-Triad Protection ai più recenti sviluppi*, *cit*., p. 460.

[195] Si rinvia alla nota 189 per la consultazione del testo di queste disposizioni.

[196] TRABACCHI, *I delitti contro la fede pubblica,* in MARINUCCI-DOLCINI (a cura di), *Trattato di diritto penale. Parte speciale*, Padova, 2011, p. 106-107, chiarisce come non si tratti né di condotte equivalenti, né si possa considerare

La ragione sostanziale di questa differenza e in generale del trattamento normativo della spendita o messa in circolazione quali delitti autonomi, può essere rintracciata nella tendenza della dottrina[197] ad individuarne il disvalore nella concretizzazione, suo tramite, degli effetti dannosi della contraffazione o dell'alterazione[198]. Per questa ragione laddove sia commessa dallo stesso autore o concorrente nella falsificazione ne costituisce post fatto non punibile[199]. Ad analoga *ratio* sembra ispirarsi anche la differente strutturazione, all'art. 453 n. 3 c.p. e all'art. 455 c.p., dei delitti d'introduzione nel territorio dello stato e di detenzione[200] commessi da terzi rispettivamente in

---

la spendita come una specificazione della immissione in circolazione, costituendola la prima "*un'ipotesi autonoma*", comportante la dazione della moneta in pagamento e la sua accettazione come genuina, ed identificandosi la seconda con ogni diversa condotta determinante il trasferimento della moneta falsa.

[197] In questo senso TRABACCHI, *op. cit.*, p. 122.

[198] LONGO, *Falso nummario e in sigilli,* in PELISSERO-BARTOLI, *Reati contro la fede pubblica*, Giappichelli, 2011, p. 14-15, definisce contraffazione la creazione di moneta non genuina per titolo, valore, forma e qualità di metallo impiegato, e l'alterazione come sua modificazione artificiosa in modo da attribuirle un valore nominale differente; in entrambi i casi deve trattarsi di falso nummario non grossolano, il quale, essendo privo della spendibilità tipica della moneta, non sarebbe punibile ai sensi dell'art. 49 comma 2 c.p., per inidoneità dell'azione. La giurisprudenza di legittimità richiede ai fini della ricorrenza delle due forme di falsificazione la previa esistenza del tipo di moneta, o di carte di pubblico credito ai sensi dell'art. 458 c.p., che sia contraffatta o alterata. In questo senso esplicita è Cass. pen., Sez. V, 10 maggio 2016, n. 19441, consultabile alla banca dati *Pluris on line*, per cui la "*contraffazione si concretizza in una imitatici veri, vale a dire nella creazione non consentita, da parte, cioè, di chi non sia autorizzato, di monete (o di carte di pubblico credito) che abbiano un'apparenza di genuinità, mentre la "alterazione" presuppone la genuinità della moneta (o della carta di pubblico credito), consistendo in una modificazione dello stato preesistente della sostanza con cui la moneta è fatta e delle caratteristiche della moneta, finalizzata a creare l'apparenza di un valore superiore o inferiore (nel qual caso ricorrerà l'ipotesi di reato di cui all'art. 454 c.p.) rispetto a quello effettivo (….) Orbene non appare revocabile in dubbio che l'attività di falsificazione definita nelle due forme della "contraffazione" e della "alterazione" presuppone necessariamente l'esistenza, nella realtà fenomenica del mondo degli scambi economici, commerciali e finanziari, di beni, rappresentati da monete o da carte di pubblico credito, effettivamente esistenti (...) mentre quando la suddetta attività si sostanzi nella creazione di una moneta o di una carta di pubblico credito sconosciuta alla realtà fenomenica ed alla storia degli scambi economici, commerciali e finanziari (anche le monete ed i titoli fuori corso, infatti, sono dotati di valore nel mercato numismatico e possono formare oggetto di contrattazioni) tale, cioè, da risultare del tutto inesistente, è altrove che va ricercata la eventuale rilevanza penale di tale condotta (che, ad esempio, potrebbe integrare gli estremi degli artifizi o dei raggiri di cui al reato di truffa previsto dall'art. 640 c.p.)".*

[199] Così VASSALLI, voce *Antefatto non punibile, post-fatto non punibile*, in *Enciclopedia del Diritto*, vol. II, 1958, p. 507 ss., il quale richiama in proposito criticamente la dottrina tedesca dei reati di utilizzazione, i quali non sarebbero altro che uno dei modi di realizzazione ordinaria del fine del reato principale. Per l'insigne Maestro nota identificativa di questa categoria e di quella confinante dell'antefatto non punibile sarebbe, invece, la presenza di condotte distinte, costituenti di per sé reato, le quali integrano diversi tipi, stadi o gradi di offesa al medesimo bene e sono avvinte tra loro da un rapporto di mezzo-fine, che sarebbe, peraltro, mancante nella progressione criminosa in senso tecnico dove il progredire dell'offesa sarebbe dipendente da risoluzione successive. Per la giurisprudenza nazionale di legittimità, tra cui di recente, con specifico riferimento alle previsione dell'art. 453, nn. 3 e 4, c.p., Cass. pen., sez. I, 10 gennaio 2020, n. 588, le disposizioni sul falso nummario sarebbero norme a fattispecie plurime, individuanti "*un fatto lesivo sostanzialmente unico, con la conseguenza che, laddove un fatto concreto integri più condotte tipiche e queste ultime vengano realizzate senza apprezzabile soluzione di continuità sul medesimo oggetto materiale, le stesse perdono la loro individualità e rimangono assorbite nella più grave di esse*".

[200] Per CINCOTTA, *Della falsità in monete, in carte di pubblico credito e in valori di bollo (artt. 453-466),* in RAMACCI (a cura di), *I delitti contro la fede pubblica - Trattato di diritto penale,* Giuffrè, 2013, p. 187- 191, il delitto d'introduzione è integrato da qualsiasi condotta che comporti il trasferimento della moneta dalla località estera in cui è stata contraffatta o alterata a quella nazionale, mentre quello di detenzione sussiste in presenza della disponibilità di fatto di moneta falsa, assumendo valore di autonoma consumazione rispetto alla spendita o

presenza e in assenza di concerto con il falsificatore o l'intermediario[201]: nel primo caso la ricorrenza di questo legame giustifica la punibilità in sé di queste condotte, che si porrebbero, in virtù del concerto, in progressione criminosa[202] rispetto alla falsificazione; mentre nelle seconde[203], così come nei delitti di acquisto e ricezione[204], costruiti sulla falsariga del delitto di ricettazione[205], sarebbe il perseguimento del fine di messa in circolazione a garantire la strumentalità alla realizzazione del "*significato e (del)la funzione del prodotto della falsificazione*"[206].

Nel raffronto con gli obblighi di incriminazione contenuti nella direttiva UE/2019/713, la questione da definire risulta, allora, stabilire se la fraudolenza sia requisito tale da "alterare" quel "*rapporto di consequenzialità logica*"[207] che collocherebbe in un contesto delittuoso unico[208] i reati "connessi" e

messa in circolazione, che consistono nell'uso "normale" della moneta e in qualsiasi altro impiego, solo se le ha precedute per un tempo apprezzabile.

[201] LONGO, *Falso nummario e in sigilli, cit*., p. 17-18, rappresenta come ai fini della ricorrenza del concerto per la giurisprudenza basta anche un'intesa momentanea, purché chi riceve le monete operi come "*longa manus*" dei contraffattori, mentre per intermediario si intende "*il ricettatore ex art. 648 c.p.*", cioè, chi "*acquista le monete falsificate non per spenderle, né per farle circolare come mezzi di pagamento, ma per rivenderle ad altri e conseguire così un profitto*".

[202] Si veda, sulla distinzione tra progressione criminosa in senso lato e progressione criminosa in senso tecnico, VASSALLI, voce *Progressione criminosa e reato progressivo*, in *Enciclopedia del Diritto*, vol. XXXVI, 1987, p. 1160, che definisce quest'ultima come quelle ipotesi di commissione, in virtù di risoluzione successive e autonome, di più violazioni quasi contestuali, in cui la successiva implica la precedente meno grave.

[203]CINCOTTA, *Della falsità in monete, in carte di pubblico credito e in valori di bollo (artt. 453-466), cit*., p. 206, le condotte di questa fattispecie corrispondono nella sostanza a quelle previste dall'art. 453, n. 3, c.p., ad eccezione dell'assenza di concerto con il falsificatore o l'intermediario, e richiedono, in virtù del dolo specifico richiesto e della previsione del differente reato di spendita di monete falsificate ricevute in buona fede, di cui all'art. 457 c.p., la consapevolezza della non autenticità della moneta già al momento in cui se ne consegue la disponibilità.

[204] Si tratta delle fattispecie -a dolo specifico di mettere in circolazione monete falsificate- di acquisto e ricezione direttamente dal falsificatore o intermediario, previste all'art. 453. n. 4 c.p., e di quella di acquisto da chiunque le detenga, punita all'art. 455 c.p. con un trattamento sanzionatorio più lieve. Per CINCOTTA, *Della falsità in monete, in carte di pubblico credito e in valori di bollo (artt. 453-466), cit*., p. 192, le condotte di acquisto e ricezione richiedono entrambe il conseguimento della disponibilità di monete contraffatte o alterate, differenziandosi l'acquisto solo per il pagamento di un prezzo. L'Autore chiarisce, anche, che la realizzazione di queste condotte in assenza del dolo specifico di circolazione ne potrà comportare, laddove sia sussistente il diverso fine di profitto, la punibilità come ricettazione

[205] Come rappresentato da LONGO, *Falso nummario e in sigilli, cit.,* p. 11-13, a questo delitto sembrano ispirarsi le fattispecie, diverse dalla contraffazione e dall'alterazione, previste dagli artt. 453-458 c.p., "*assimilate quoad poenam alla falsificazione*" ed accomunate dal presupposto negativo che il soggetto agente non debba rispondere a titolo di concorso ex art. 110 c.p. nel reato di contraffazione o di alterazione.

[206] Così TRABACCHI, *I delitti contro la fede pubblica, cit.*, p. 125.

[207] Testualmente, con riferimento al legame intercorrente tra il reato presupposto e i reati di ricettazione e favoreggiamento, MORGANTE, *Il reato come elemento del reato. Analisi e classificazione del concetto di reato richiamato dalla fattispecie penale*, Giappichelli, 2013, p. 75, la quale chiarisce che questo nesso corrisponde a quello sussistente tra le fattispecie d'impiego del falso e la falsificazione, con la differenza che in questo caso i reati presupposto sono specificatamente individuati.

[208]In questi termini MORGANTE, *Il reato come elemento del reato. Analisi e classificazione del concetto di reato richiamato dalla fattispecie penale*, *cit*., p. 76-77, per cui "*il reato accessorio è strutturalmente un postfatto non punibile nei casi di concorso nel reato precedente*".

quello di utilizzazione, consentendo l'incriminazione autonoma di quest'ultima condotta anche laddove commessa dallo stesso autore[209].

Per rispondere a questo quesito bisogna, prima di tutto, definire la nozione di fraudolenza.

A questo proposito non sembra possibile sostenerne una ricostruzione in termini solo modali, quale necessità dell'impiego di mezzi fraudolenti[210], poiché si tratterebbe di un requisito, da un lato, superfluo rispetto a quegli strumenti di pagamento che, in quanto contraffatti, avrebbero di per sé una carica di tal fatta, dall'altro, generativo di sovrapposizione con il delitto di truffa, che è, peraltro, ritenuto dalla giurisprudenza nazionale suscettibile di concorso con il delitto di spendita o messa in circolazione di moneta falsa[211].

Nonostante quanto sopra, non sarebbe, però, nemmeno opportuno concepire la fraudolenza come mero intento di frode a valenza esclusivamente soggettiva che dovrebbe animare l'agente[212] e che,

---

[209] In questo senso, relativamente alle fattispecie nazionali di ricettazione e favoreggiamento, PROSDOCIMI, *Profili penali del post fatto,* Giuffrè, 1982, p. 187, che discorre di "*frantumazione del concorso successivo nel reato- o, per meglio dire, quello che tale avrebbe altrimenti potuto essere- in una serie di fattispecie autonome. Ciò che per l'intraneo nel reato pregresso rientra nel quadro valutativo di tale reato; per l'estraneo dà vita ad un reato nuovo*".

[210] In questo senso con riferimento al reato di false comunicazioni sociale, nella versione precedente alla modifiche apportate dopo il d.lgs. n. 61/2002, GAMBARDELLA, *Il significato e il contenuto dell'avverbio fraudolentemente nel reato di false comunicazioni sociali (art. 2621, n. 1, c.c.)*, in *Cass. pen*., 9/1998, p. 2532-2533, il quale rappresenta, indipendentemente dalle specifiche regioni attinenti la fattispecie esaminata, come una concezione di questo tipo debba essere esclusa perché conseguente a quella tendenza della dottrina e giurisprudenza a concepire in termini meramente soggettivi quegli atteggiamenti interiori in funzione tipizzante la condotta materiale.

[211] Così Cass. pen., Sez. II, 16-12-2019, n. 50697, consultabile alla banca data *Pluris on line*, che, concependo il reato di spendita di monete false reato istantaneo di pericolo a tutela della pubblica fede, ammette il concorso con il delitto di truffa se dalla sua realizzazione deriva all'agente anche un ingiusto profitto con danno patrimoniale altrui: "*Non appaiono, pertanto, condivisibili né il principio secondo cui la norma penale che prevede la spendita di moneta falsa (artt. 453 e 455 c.p.) è norma speciale rispetto a quella che prevede il reato di truffa poiché il primo delitto contiene tutti gli elementi del secondo con l'apporto di un elemento specializzante costituito dall'uso di moneta falsa come mezzo per trarre in inganno e si avrebbe, quindi, assorbimento della norma generale in quella speciale ex art. 15 c.p. e non concorso formale di reati (vedi Sez. 5, n. 5197 del 10/12/1976 - dep. 22/04/1977, COSTANZA, Rv. 13567001) né il principio secondo cui nel caso di spendita di monete false (art. 455 c.p.) la tutela della fede pubblica inerente alla regolare circolazione delle monete assorbe la tutela della buona fede individuale e del patrimonio di cui all'art. 640 c.p. (vedi Sez. 5, n. 8091 del 09/01/1976 - dep. 16/07/1976, RICEPUTI, Rv. 13413901). Ed, invero, la consegna di moneta falsa ad un terzo in occasione di una transazione commerciale comporta chiaramente un danno patrimoniale a chi la riceve in buona fede con correlativo ingiusto profitto da parte di colui il quale la consegna, realizzandosi, oltre che l'offesa alla fede pubblica, la lesione patrimoniale che, in quanto determinata da un raggiro, integra il reato di truffa.*" E' in dottrina di contrario avviso sul punto TRABACCHI, *I delitti contro la fede pubblica, cit.*, p. 135, per cui "*spende soltanto chi dà moneta in pagamento come se fosse genuina (…) Neppure è vero che «la spendita prescinde dall'ingiusto profitto e dal danno patrimoniale» richiesti invece per la truffa: senza ingiusto profitto, senza danno, senza induzione in errore non può darsi spendita, ma soltanto immissione in circolazione*".

[212] Rispetto ad uno strumento di pagamento, ad es. rubato, il requisito della fraudolenza non può non avere una valenza oggettiva che renda materialmente percepibile quella carica di disvalore che contrassegna l'utilizzazione rispetto al furto e che si rivolge ad interessi diversi da quelli del singolo individuo pregiudicato dalla sottrazione. Per una concezione in termini oggettivi della locuzione avverbiale in esame con riferimento al delitto di intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche vedi SALVADORI, *I reati contro la riservatezza informatica*, in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime*, *cit*., p. 709, il quale discorre "*di condotte di intercettazione che, da un punto di vista oggettivo, si realizzino in modo occulto e con modalità particolarmente insidiose, in modo tale da non rendere riconoscibile l'intromissione*

anche in considerazione dell'immaterialità del possibile sostrato di riferimento, sarebbe di difficile accertamento.

Sembra evitare gli eccessi di entrambi queste ricostruzioni (requisito modale o finalistico) la considerazione della fraudolenza come elemento normativo, con riflesso anche soggettivo, del fatto tipico[213], da riferire agli effetti che la condotta dovrebbe provocare rispetto a terzi, che dovrebbero rimanere ignari dell'illiceità o falsità dello strumento.

In questo modo questo requisito risulterebbe, da un lato, rafforzativo della specifica connotazione illecita del suo oggetto, che dovrà necessariamente essere sussistente, e, dall'altro, compatibile solo con un atteggiamento soggettivo di consapevole volontà di "sfruttarla". Una visione di questo tipo ha il pregio di proiettare sul piano della tipicità una carica offensiva compatibile con la prospettiva di tutela della sicurezza del mercato, adottata dal legislatore europeo.

Questa carica, pur potendo essere considerata come la concretizzazione o l'aggravamento della portata dannosa della condotta a monte, sembra "ulteriore", manifestando, soprattutto con riferimento agli strumenti di derivazione illecita "genuini" ed in considerazione delle concrete modalità di realizzazione, un'offensività propria.

Sul punto il legislatore europeo si limita a riconoscere agli Stati membri la facoltà che "*qualora un reato di cui alla presente direttiva sia stato commesso, in connessione con un altro reato di cui alla presente direttiva da parte della stessa persona, e uno di tali reati di fatto costituisce un elemento necessario del primo reato in questione, gli Stati membri possono, conformemente ai principi generali del diritto nazionale, prevedere che tale condotta sia considerata circostanza aggravante del reato principale*"[214].

---

abusiva da parte del soggetto passivo". *Contra* PLANTAMURA, *La tutela penale delle comunicazioni informatiche e telematiche*, in *Dir. informatica*, 6/2006, p. 847 ss., per cui, invece, "*il "fraudolentemente", quindi, serve solo ad escludere dalla penale rilevanza le intercettazioni occasionali: ovvero le intercettazioni volontarie, che sono frutto, però, di circostanze non preordinate dal soggetto agente, come, ad es., nel caso di chi decida di sfruttare una casuale interferenza*".

[213] In termini analoghi GAMBARDELLA, *Il significato e il contenuto dell'avverbio fraudolentemente nel reato di false comunicazioni sociali (art. 2621, n. 1, c.c.)*, *cit*., p. 2538, che con riferimento a questo delitto, nella versione precedente alla modifiche apportate dopo il d.lgs. n. 61/2002, discorre di intenzione fraudolenta che nel sorreggere l'occultamento di fatti societari rilevanti o l'esposizione di quelli falsi contribuisce a tipizzare anche oggettivamente la condotta criminosa. In questo senso, nonché per gli orientamenti giurisprudenziali sorti sulla ricostruzione di questo requisito, si rinvia a CRESPI, *Rassegna di diritto societario (1999-2000) Disposizioni penali in materia di società e consorzi*, in *Riv. soc*., fasc.2-3, 2002, p. 630 ss.; nella prospettiva anche di raffronto rispetto ai successivi interventi riformatori vedi DONINI, *Abolitio criminis e nuovo falso in bilancio struttura e offensività delle false comunicazioni sociali (artt. 2621 e 2622 c.c.) dopo il d.lg. 11 aprile 2002, n. 61*, in *Cass. pen*., 4/2002, p. 1240 ss..

[214] In questi termini il considerando 19 della direttiva UE/2019/713.

Una disposizione simile è già prevista nel nostro ordinamento, come circostanza aggravante comune all'art. 61 n. 2 c.p., con riguardo all'esecuzione del reato per eseguirne od occultarne un altro o per assicurarsene il prodotto, il profitto o il prezzo ovvero l'impunità[215].

Questa disposizione è considerata espressione di quel fenomeno- inerente alle dimensione fattuale delle manifestazioni criminose- definito come "*connessione di reati*" e sussistente quando "*tra gli elementi delle più fattispecie concrete ve ne siano alcuni comuni o interdipendenti*"[216].

Nonostante l'apparente corrispondenza della connessione così definita con quella oggetto degli obblighi d'incriminazione sovranazionali, la disciplina dell'art. 61 n. 2 c.p. non può costituire la soluzione legislativa nazionale di riferimento, in quanto ordinariamente considerata espressione della particolare attitudine criminosa del reo in relazione al singolo reato funzionalmente connesso[217]. Una declinazione nazionale di questo tipo degli obblighi d'incriminazione in esame finirebbe, infatti, per svilire l'autonomia prima di tutto materiale, oltre che eventualmente offensiva, della condotta di utilizzazione, pur nella sua "dipendenza" dalla condotta fonte del suo oggetto, nonché di quest'ultima e di quelle intermedie.

Ad avviso di chi scrive, soluzione normativa conforme a quanto sopra rappresentato potrebbe essere, invece, la previsione dell'utilizzazione e delle condotte connesse in un'unica "disposizione a più norme", che individui non alternativamente, ma cumulativamente più ipotesi di reato[218].

---

[215]La predetta disposizione considera tre situazioni diverse tra loro, definite rispettivamente nesso teleologico, nesso paratattico e nesso ipotattico. Per l'analisi particolareggiata di ciascuna delle tre ipotesi si rinvia a FRAGASSO, VERGINE, *sub Art. 61*, in DOLCINI-GATTA, Codice penale commentato, Tomo I, V ed., 2021, p. 1236-1237, che evidenziano come "*il fondamento razionale di tale aggravante sia discutibile per molteplici ragioni. Tra queste il fatto che esistano reati che per propria natura non sono fini a se stessi (per es. i falsi); il fatto che ben spesso il reato mezzo è il modo consueto per realizzare il reato-fine; il fatto che il reato-fine rappresenta una sorta di naturale sbocco del reato-mezzo. Del resto, le frequentissime controversie cui l'applicazione dell'aggravante ha dato luogo sono la prova del deficit di razionalità che la caratterizza ed il fatto che, in passati progetti di riforma del codice penale, la suddetta aggravante non venisse più contemplata, pare significativo dello scarso apprezzamento di cui la stessa oggi gode anche a causa del suo "indistinto ed indiscriminato rigore*".

[216] In questi termini LAPICCIRELLA, *voce Connessione (dir. proc. pen.),* in *Enciclopedia del Diritto*, vol. IX, 1961, p. 33-34, il quale rappresenta come la connessione di reati sia dal punto di vista processuale anche una connessione materiale che determina l'unificazione dei procedimenti e comporta effetti pregiudiziali, in termini d'influenza del giudicato sul procedimento connesso.

[217] In questo senso FRAGASSO, VERGINE, *op. ult. cit*.; in giurisprudenza si esprime in questi termini anche Cass. pen., sez. V 12 ottobre 2020, n. 34504; Cass. pen. sez. V, 26 novembre 2019, n. 22; Cass. pen., sez. V, 06 novembre 2017, n. 57488, tutte consultabili alla banca dati *Pluris on line*.

[218] Sul fenomeno generale delle fattispecie legali miste, alternative o cumulative, cfr. VASSALLI, *Le norme penali a più fattispecie e l'interpretazione della legge Merlin*, in *Studi in onore di F. Antolisei*, III, Giuffrè, 1965; specificatamente sulla definizione di "disposizione a più norme" come contenente tante norme incriminatrici quante sono le fattispecie legislativamente previste si rinvia a COCCO, *Reato istantaneo, di durata e a più fattispecie. Questioni controverse di unità e pluralità*, in *Responsabilità civile e previdenza*, 2/2017, p. 393, che contrappone questa categoria a quella di "norma a più fattispecie" in cui, nonostante siano tipizzati più comportamenti si tratta di una sola norma, essendo questi comportamenti indifferentemente offensivi dello stesso bene giuridico. Circa la predetta denominazione di "disposizione a più norme" si precisa che è stata volutamente adottata rispetto ad altra formulazione per il significato che la nozione di disposizione ha rispetto al concetto di norma; su questo significato cfr. DONINI, *Il diritto giurisprudenziale penale. Collisioni vere e apparenti con la*

Rispetto a queste ipotesi la connessione potrebbe, comunque, essere foriera di conseguenze, ancorché non "unificanti" o semplicemente "aggravanti", incidenti sul livello di colpevolezza attribuibile al reo e sul connesso trattamento sanzionatorio irrogabile.

Quanto sopra sarebbe, in particolare, possibile in conseguenza della considerazione, ai fini del trattamento sanzionatorio di favore previsto dall'art. 81 c.p.[219], di quel rapporto di mezzo- scopo[220] che leghi i reati connessi, che siano stati commessi dal medesimo soggetto autore poi dell'utilizzazione, analogamente al finalismo tipico dei reati in continuazione[221].

3.1 Il fine di utilizzazione fraudolenta

Con riferimento alle altre condotte oggetto degli obblighi d'incriminazione, successive a quelle fonte dell'oggetto dell'utilizzazione, ma prodromiche rispetto a quest'ultima- quali l'atto di procurare per sé o per altri strumenti di pagamento materiali o immateriali falsificati o di origine illecita, il possesso o la detenzione di strumenti di tal fatta-il legame di mezzo-scopo assume, invece, già nella prospettazione sovranazionale una valenza strutturale, incidente direttamente sul fatto tipico.

---

legalità e sanzioni dell'illecito interpretativo, in *Diritto penale contemporaneo Rivista trimestrale*, 3/2016, p. 6-7, che definisce la disposizione come enunciato normativo da cui estrarre, mediante l'interpretazione o in virtù della sua applicazione ai casi, il contenuto sostanziale costituito dalla norma.

[219] Sul concorso di reati in generale ed in particolare sulla disciplina posta per questa tipologia di concorso cfr. PROSDOCIMI, *Concorso di reati e di pene*, in *Digesto pen.*, II, Torino, 1988, 508 ss.; per PAGLIARO, *voce Concorso di reati*, in *Enc. Dir.*, VIII, Milano, 1961, p. 669, il concorso formale, al pari della continuazione, riguarderebbe le ipotesi di realizzazione a struttura unitaria di una pluralità di reati e sarebbe per questo espressione di una minore riprovevolezza complessiva.

[220]Per SOTIS, *Il ''concorso materiale apparente'': confine tra artt. 15 e 81 c.p.*, in *Giur. it.*, gennaio 2020, p. 193, l'art. 81 c.p. proprio perché garantisce "*la proporzionalità tra gravità del fatto e pena (il parametro del giudizio)*" consente "*valutazioni di tipo non strutturale (il metodo del giudizio), come l'offesa anzitutto, poi il rapporto tra mezzi e scopo, l'idquod plerumque accidit, l'immediatezza e lo scopo unitario che anima la volontà dell'agente. E queste valutazioni debbono necessariamente osservare il mondo dei fatti (l'oggetto del giudizio) in raffronto con le fattispecie incriminatrici, perché è da questo raffronto che emerge l'eventuale sproporzione tra la pena comminata per ogni singolo reato, in caso di realizzazione solo di quel reato, e quella emergente a seguito della commissione di un fatto in cui si registrano sovrapposizioni, e doppie (o triplici) valutazioni di elementi e di offese commessi nella realtà una sola volta*".

[221] A favore dell'espressione continuazione anziché "reato continuato" cfr. PAGLIARO, *Il reato, cit.*, p. 604; BRUNELLI, *Dal reato continuato alla continuazione di reati: ultima tappa e brevi riflessioni sull'istituto*, in *Cass. pen.*, 7-8/2009, 2749 ss.; CAPUTO, *Dalla disintegrazione del reato continuato alla continuazione di reati. Osservazioni in ordine al calcolo dell'aumento di pena*, in *Cass. pen.*, 3/2016, p. 1052 ss.. Sull'origine e *ratio* di questo istituto si rinvia a ZAGREBELSKI, *voce Reato continuato*, in *Enc. Dir.*, XXXVIII, Milano, 1987, p. 839 ss., il quale propende per la sua natura sostanzialmente pluralistica e ne ammette la coesistenza con l'aggravante dell'art. 61, n. 2, c.p., riguardando quest'ultima il singolo reato e non il complesso di reati. Di recente, in termini analoghi anche PANEBIANCO, *La persistente vivacità del reato continuato nella giurisprudenza delle Sezioni Unite*, in *Giur. it.*, marzo 2019, p. 694, per cui l'art. 81 c.p. "*darebbe veste unitaria ad un concorso materiale di reati ai soli fini della determinazione del trattamento sanzionatorio*".

In particolare, il dolo specifico di utilizzazione fraudolenta indicato dal legislatore europeo non è né generativo, né tantomeno dirimente di un possibile concorso di reati, ma indicativo di una particolare "*definizione in termini penalistici di un requisito strutturale di un illecito unitario*"[222].

La sua previsione sembra, infatti, considerabile alla stregua di una clausola di strumentalizzazione espressa in funzione "tipizzante" del contenuto oggettivamente lesivo delle condotte da incriminare: lo scopo di "*intraprendere, dopo la condotta-base, attività ulteriori, implica non soltanto la loro previa rappresentazione, da parte dell'agente, ma anche che questa abbia efficacia causale (sia pur non esclusiva) sull'azione esterna, configurandola come esecutiva di un'unica "globale" volontà di agire (…) momento necessario al pieno verificarsi del risultato "finale" tipicamente perseguito o all'intrapresa delle successive attività avute di mira, come descritte dalla norma*"[223].

Come è stato autorevolmente messo in luce con riferimento alle fattispecie nazionali di acquisto e ricezione di moneta contraffatta rispetto al fine di messa in circolazione, la predetta efficacia causale del fine non è, però, concepibile come "*idoneità "causale" della condotta base al compimento del secondo atto c.d. «incompiuto» (il mettere in circolazione), dipendendo la realizzazione di questo da un'autonoma e successiva determinazione di volontà dell'agente o addirittura di terzi*"[224]. Per questa dottrina il dolo specifico va inteso come "*causa anche psichica*"[225] che muove l'agente a porre in essere quelle modalità tassativamente indicate, oggettivamente strumentali alla realizzazione di un'attività ulteriore e distinta, a prescindere dalla prossimità o dal grado di probabilità della verificazione[226].

---

[222] Testualmente MORGANTE, *Il reato come elemento del reato. Analisi e classificazione del concetto di reato richiamato dalla fattispecie penale*, *cit*., p. 128, che rappresenta come nel dolo specifico di reato quest'ultimo rileva quale "*fonte di qualificazione penalistica*" di un elemento della fattispecie.

[223] Testualmente PICOTTI, *Il dolo specifico. Un'indagine sugli "elementi finalistici" delle fattispecie penali*, Giuffrè, 1993, p. 501-502; L'Autore a p. 585 precisa come "*la tecnica di formulazione imperniata sul mezzo-fine, pur comportando un'anticipazione del momento consumativo ad uno stadio antecedente il materiale conseguimento del risultato avuto di mira dal reo, non implica necessariamente anche una "psicologizzazione" del reato, perlomeno nel senso di una confusione fra la delimitazione della sua tipicità oggettiva e il momento della sua imputazione e rimproverabilità soggettiva a titolo di dolo, fondandosi su presupposti propriamente "soggettivi", nel senso di psicologici e personali*".

[224] Così PICOTTI, *Il dolo specifico. Un'indagine sugli "elementi finalistici" delle fattispecie penali*, cit., p. 510; sullo schema tipico di realizzazione del delitto a due atti incompiuto vedi anche p. 254.

[225] In questi termini PICOTTI, *op. cit*., p. 514 che precisa che il fine è configurato "*quale elemento che effettivamente attiva la realizzazione strumentale "esterna": non quale risultato, che le forze causali attivate dall'agente devono materialmente (poter) produrre*". *Contra* MARINO, *Il "filo di Arianna". Dolo specifico e pericolo nel diritto penale della sicurezza*, in *Diritto penale contemporaneo Rivista trimestrale*, 6/2018, p. 63 per cui, invece, "*se non è necessario che l'oggetto del dolo specifico si realizzi, è evidente che sia proprio la connessione materiale-teleologica tra fatto e scopo a rilevare ai fini della concreta costituzione di un pericolo per il bene di riferimento, riverberandosi in senso eziologico sulla condotta, alla stregua dei giudizi di idoneità e univocità propri del modello del delitto tentato*".

[226] Per PICOTTI, *op. cit*., p. 515-516, "*nei reati a dolo specifico non essendovi traccia dei requisiti di idoneità ed univocità (oggettive) degli atti di "esecuzione" rispetto alla realizzazione del risultato, che è posto a contenuto del fine dell'agente, il momento consumativo corrisponde sempre e solo a quello dell'integrazione della condotta o fatto-base "strumentali", tassativamente descritti dalla fattispecie, non diversamente che in ogni altro reato di condotta o ad evento*", mentre nel delitto tentato "*il momento di "perfezione" appare determinabile solo attraverso un concreto giudizio per relationem, di prossimità o "pericolosità" oggettive (idoneità), rispetto all'iter esteriormente proiettato (univocità) alla realizzazione o produzione del risultato finale lesivo, vietato dalla singola norma incriminatrice*".

Questa autorevole ricostruzione dogmatica è da preferire rispetto a quella tendenza a qualificare criticamente condotte, analoghe a quelle di cui agli obblighi d'incriminazione in esame, come modalità tipiche del diritto penale della prevenzione[227] costituenti mere fattispecie ostative[228] subiettivizzate[229], in cui l'elemento soggettivo richiesto sarebbe analogo a quello del delitto tentato ma riferito a meri atti preparatori di per sé inoffensivi[230].

Una tesi di questo tipo, oltre ad annullare la diversità strutturale dei reati a dolo specifico rispetto al tentativo[231], disconosce la carica di disvalore che è insita nella "*perdurante disponibilità*" di un oggetto criminale quale "*antecedente logico-criminologico, di un concorso formale o materiale di reati-fine*"[232], la cui incriminazione dovrebbe operare in funzione disincentivante sia per il detentore, sia per i terzi dall'impiego della *res illicita*[233].

Non tiene, inoltre, conto del fatto che è proprio la proiezione finalistica a colorare offensivamente la condotta incriminata per la sua strumentalità rispetto ad un successivo pregiudizio[234].

---

[227] In questo senso M. MANTOVANI, *La struttura dei reati di possesso,* in www.dirittopenalecontemporaneo.it, del 7 novembre 2012, p. 1, per cui "l*a spiegazione politico-criminale del crescente ricorso a questa tipologia di incriminazioni risiede nell'essere il possesso – rectius la detenzione, per darne una definizione più ampia e insuscettibile di essere imbrigliata dalle contaminazioni e dalle problematiche che l'accostamento alla nozione civilistica di possesso può comportare di determinati oggetti sia il risultato di reati precedentemente commessi (dallo stesso detentore o da terzi, in concorso o meno con lui); sia, anche e soprattutto, il prodromo rispetto alla commissione di (ulteriori) futuri reati*".

[228] In generale sulla ricostruzione di questa categoria come punizione di quelle condotte base per la realizzazione di altri reati *cfr.* PAGLIARO, *Il reato*, cit., p. 34; sull'esame specifico di alcuni reati nazionali di possesso e detenzione con un fine specifico vedi SALVADORI, *I reati di possesso. Un'indagine dogmatica e politico-criminale in prospettiva storica e comparata*, Edizioni Scientifiche Italiane, Napoli, 2016, p. 261 ss.; con specifico riferimento alla condotta di possesso incriminata, oggi, dalla seconda parte del primo comma dell'art. 493 ter c.p. si rinvia a ZACCAGNINI, *Note sull'art. 12 della l. 197/91, quale "disposizione di chiusura" della normativa di compliance italiana e suoi rapporti con il delitto di ricettazione*, in *Cass. pen.*, 1/2002, p. 323, il quale rappresenta come questa condotta sia un reato ostativo a condotta neutra e a dolo specifico di profitto con il quale viene incriminato un momento anteriore e prodromico all'abuso di carta di pagamento.

[229] Così MONGILLO, *Il principio di offensività tra costituzionalizzazione e codificazione*, in *Giur. mer.*, 2002, p. 1169-1170, che qualifica altresì questi ipotesi come reati a dolo specifico di offesa, tra cui include anche l'acquisto di monete contraffatte al fine di metterle in circolazione, e ne ammette l'impiego, date le insuperabili frizioni con il principio di offensività, solo in presenza d'interessi fondamentali e laddove ne sia empiricamente comprovata l'idoneità preventiva.

[230] In questi termini MONGILLO, *Il principio di offensività tra costituzionalizzazione e codificazione*, *cit.*, p. 1168, il quale considera i reati ostativi come irrimediabilmente senza offesa, trattandosi di atti che ne costituiscono semplicemente la premessa idonea e che sono carenti, anche, sotto il profilo dell'univocità.

[231] Vedi nota 226.

[232] Testualmente M. MANTOVANI, *La struttura dei reati di possesso, cit.*, p. 11, il quale concepisce la detenzione di monete falsificate un reato-mezzo a natura permanente, che sarebbe soggetto allo stesso trattamento sanzionatorio della spendita o messa in circolazione in virtù della circostanza che è la perdurante disponibilità di tali monete a consentire la possibile reiterazione delle successive condotte di spendita o messa in circolazione.

[233] COSÌ SALVADORI, *I reati di possesso. Un'indagine dogmatica e politico-criminale in prospettiva storica e comparata*, *cit.*, p. 412-413.

[234] ZACCAGNINI, *Note sull'art. 12 della l. 197/91, quale "disposizione di chiusura" della normativa di compliance italiana e suoi rapporti con il delitto di ricettazione*, *cit.*, p. 326.

Quanto sopra vale anche per le condotte di possesso o di detenzione di cui agli obblighi d'incriminazione in esame, in cui la proiezione finalistica rispetto ad un'attività futura risulta ben delineata e distinta dal fatto base, il quale a sua volta appare munito della necessaria determinatezza[235]. In proposito, ancorché con riferimento alla sola condotta di detenzione, va considerata con favore la previsione espressa dell'ulteriore requisito intellettivo della rappresentazione dell'origine illecita, la quale contribuisce ulteriormente, in una visione teleologica integrata degli elementi oggettivi e soggettivi del reato[236], alla descrizione del "*significato lesivo dell'intero fatto come descritto dalla fattispecie legale*"[237].

[235] In termini analoghi con riguardo alle fattispecie a dolo specifico in generale PICOTTI, *op. cit.*, p. 519.
[236] GALLO, *Il dolo. Oggetto e accertamento*, Giuffrè, 1953, p. 262, mette in chiaro proprio con riferimento alla ricezione di monete false che la sua rilevanza penale è condizionata dall'intento di mettere in circolazione a conferma di come il disvalore del fatto sia dipendente anche dai suoi coefficienti soggettivi.
[237] PICOTTI, *op. cit.*, p. 559, che evidenzia, inoltre, come in una visione unitaria del fatto tipico "*non è il fine in quanto tale ad incidere sul contenuto di offesa del reato, bensì l'oggettivo significato del perseguimento- tramite la condotta- del corrispondente interesse "causale", o di parte*".

Capitolo IV

La tutela penale delle valute virtuali nell'ordinamento nazionale

Sommario: 1.Prime considerazioni sullo schema del decreto legislativo di attuazione della direttiva UE/2019/713; 2. Il raffronto con le fattispecie nazionali; 2.1. Al cospetto del delitto di furto; 2.1.2. In prospettiva *de iure condendo*; 2.2 Al cospetto del delitto di appropriazione indebita; 3. L'utilizzazione senza diritto e a vantaggio proprio o altrui e il possibile corrispondente nazionale; 3.1 Il delitto d'indebito utilizzo di strumenti di pagamento diversi dai contanti in rapporto all'utilizzazione fraudolenta; 3.2 Le altre fattispecie dell'art. 493 ter c.p. e la tecnica di normazione prescelta; 3.3 Il delitto di frode informatica: possibili modifiche superflue in prospettiva di tutela della sicurezza informatica; 3.4 Questioni problematiche irrisolte; 3.5 Questioni problematiche future.

1. Prime considerazioni sullo schema del decreto legislativo di attuazione della direttiva UE/2019/713.

In ritardo rispetto al termine di recepimento[238], l'Italia si accinge prossimante a dare attuazione alla direttiva UE/2019/713 relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti. E', infatti, in corso l'iter di approvazione dello schema del decreto legislativo[239] con cui il Governo ha esercitato la delega conferitagli con la legge di delegazione europea 2019-2020[240] per l'attuazione di questa direttiva.

In particolare, sulla base di questo schema di decreto, le modifiche[241] al tal fine indicate consistono nell'emendamento, da un lato, dell'oggetto delle diverse fattispecie dell'art. 493 ter c.p. e del regime circostanziale del delitto di frode informatica, e nell'introduzione, dall'altro, di un neo delitto di detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti, da prevedere all'art. 493 quater.

Risulta come- al fine specifico di dare copertura alle condotte illecite aventi ad oggetto strumenti di pagamento completamente dematerializzati[242]- siano previsti correttivi solo a carattere estensivo

[238] Ai sensi dell'art. 20 della direttiva UE/2019/713 il termine per conformarsi è scaduto il 31 maggio 2021.
[239] Si tratta dell'atto di Governo n. 271 che il consiglio dei Ministri del 29 luglio 2021 ha approvato in esame preliminare e che è stato trasmesso alle commissioni parlamentari per l'acquisizione dei pareri del caso.
[240] Si tratta della legge 22 aprile 2021, n. 53 con cui il Governo è stato delegato a dare attuazione a 39 direttive europee.
[241] Lo schema del decreto in esame prevede anche l'introduzione di oneri di trasmissione da parte del Ministero della giustizia alla Commissione Europea d'informazioni sull'implementazione della direttiva e sui dati statistici inerenti i procedimenti penali e le indagini relativi agli strumenti di pagamenti diversi dai contanti, nonché la regolamentazione della procedura per scambio d'informazioni con le autorità degli Stati membri, con designazione pure dell'organo nazionale competente.
[242] In questi termini la relazione illustrativa allo schema del decreto, consultabile nella sezione "*atti del Governo sottoposti a parere*" del sito istituzionale della Camera dei deputati, p. 1.

della portata precettiva di quella che è definita come "*norma "quadro" in materia di mezzi di pagamento diversi dai contati*"[243], l'art. 493 ter c.p. Per il resto, sono considerate "*le condotte dirette ad ottenere illecitamente uno strumento di pagamento immateriale diverso dai contanti già sanzionate dagli artt. 615 ter, 617 quater e 617 sexies c.p., laddove esse comportano un accesso o un'interferenza illecita rispetto ai sistemi di informazione o ai dati informatici in essi esistenti e l'intercettazione illecita di trasmissioni di dati informatici*"[244].

Venendo ad una prima analisi dei contenuti dello schema del decreto, con riferimento all'art. 493 ter c.p. contempla l'introduzione, accanto "*alle carta di credito o di pagamento ovvero a qualsiasi documento analogo abilitante al prelievo di denaro contante o all'acquisto di beni o alla prestazioni di servizi*"[245], degli strumenti di pagamento immateriali[246], con conseguente adeguamento anche della rubrica[247].

Rispetto a questa disposizione a previsione invariata, la funzione di pagamento- quale fattore identificativo determinante- era stata valorizzata in giurisprudenza per ritenere, comunque, possibile la ricorrenza della condotta di indebito utilizzo anche nell'impiego in sé del numero identificativo e dei codici del mezzo di pagamento, a prescindere dalla detenzione del supporto materiale[248]. Muovendosi nel solco di questo orientamento, soluzione analoga è stata riferita in

---

[243] In questi termini la relazione illustrativa, *cit.*, p. 2.

[244] Testualmente la relazione illustrativa, *cit.*, p. 3.

[245] La previsione di chiusura di "*qualsiasi documento analogo*" è stata concepita come formulazione idonea a ricomprendere tutti gli strumenti che, a prescindere della denominazione e dalle loro peculiarità, consentono le medesime attività possibili con le carte espressamente nominate; in questo senso D'AGOSTINO, *La tutela penale dei mezzi di pagamento della terza generazione*, in D'AMATO (a cura di), *Trattato di diritto penale dell'impresa*, Cedam, 1993, p. 405. Nella giurisprudenza di legittimità nella medesima direzione, anche, Cass. pen., Sez. IV, 21.01.2020, n. 13492 e Cass. pen., Sez. II, 30.10.2019, n. 50395, entrambe consultabili alla banca dati *Pluris on line*.

[246] L'art. 1 dello schema del decreto in esame, recependo sul punto alla lettera la direttiva UE/2019/713, contempla cosa si intende per «*strumento di pagamento diverso dai contanti*», per «*dispositivo, oggetto o record protetto*», per «*mezzo di scambio digitale*», nonché per «*valuta virtuale*». Per l'esame di queste definizioni si rinvia alle note 164 e 165.

[247] Si riporta di seguito il testo dell'art. 493 ter c.p., coordinato con le modifiche previste dallo schema di decreto in esame: "*Chiunque al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, strumenti di pagamento immateriali, carte di credito o di pagamento, ovvero qualsiasi altro strumento o documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, è punito con la reclusione da uno a cinque anni e con la multa da 310 euro a 1.550 euro. Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per altri, falsifica o altera strumenti di pagamento immateriali, carte di credito o di pagamento, ovvero qualsiasi altro strumento o documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, ovvero possiede, cede o acquisisce tali strumenti, carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi. In caso di condanna o di applicazione della pena su richiesta delle parti a norma dell'articolo 444 del codice di procedura penale per il delitto di cui al primo comma è ordinata la confisca delle cose che servirono o furono destinate a commettere il reato, nonché del profitto o del prodotto, salvo che appartengano a persona estranea al reato, ovvero quando essa non è possibile, la confisca di beni, somme di denaro e altre utilità di cui il reo ha la disponibilità per un valore corrispondente a tale profitto o prodotto. Gli strumenti sequestrati ai fini della confisca di cui al secondo comma, nel corso delle operazioni di polizia giudiziaria, sono affidati dall'autorità giudiziaria agli organi di polizia che ne facciano richiesta*". Per la consultazione del testo in vigore si i rinvia alla nota 190.

[248] Cass. pen., sez. II, 9.9.2015 n. 48044, conforme Cass. pen. sez. II, sentenza 12.12.2018 n. 55438 con nota di SCARCELLA, *L'uso dei codici di una carta di credito, senza possesso della stessa, non è frode informatica*, in *Quotidiano Giuridico* del 16.1.2019.

dottrina anche agli "*indebiti utilizzi delle chiavi crittografiche private utilizzate per trasferire valute virtuali dai portafogli digitali. Le chiavi in argomento possono porsi in connessione funzionale con l'acquisto di beni o servizi presso soggetti che accettino su base convenzionale tale modalità solutoria*"[249]. Pur condividendo la ratio di questa tesi, è innegabile, però, che i concetti di carta e documento richiamino la fisicità del mezzo[250]; per questa ragione l'inclusione espressa di cui allo schema dal decreto in esame risulta soluzione opportuna ed idonea a consentire, inoltre, l'incriminazione della falsificazione, che, a disposizione invariata, non sarebbe punibile né secondo le previsioni del falso nummario[251], né secondo quelle relative al documento informatico[252].

Giudizio in parte differente sembra, invece, riferibile al delitto da prevedere al nuovo art. 493 quater, che, nel tentativo di dare attuazione agli obblighi d'incriminazione aventi ad oggetto quelli che, secondo la terminologia europea, costituirebbero i "*mezzi utilizzati per commettere reati*"[253], dovrebbe punire con la reclusione sino a due anni e nella multa sino a 1.000 euro le condotte- che devono essere realizzate al fine di farne uso o di consentire ad altri di farne uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti- di procurarsi per sé o per altri, produrre, importare, esportare, vendere, trasportare, distribuire, mettere a disposizione apparecchiature, dispositivi o programmi informatici "*progettati al fine principale*" indicato o "*specificamente adattati al medesimo scopo*".

Riservando al prosieguo l'analisi nel dettaglio dei suoi elementi costitutivi, in prima battuta si evidenzia come, diversamente dall'art 7 della direttiva[254], lo schema del decreto riferisca una fattispecie di questo tipo genericamente ai reati riguardanti strumenti di pagamento; questa scelta, seppur apprezzabile nel tentativo di evitare selezioni tipologiche che possano essere parziali o ben

---

[249] Così DI VIZIO, *Gli obblighi antiriciclaggio per operatori in valute virtuali*, Relazione al Seminario "*Monitoraggio del flussi finanziari e delle attività commerciali al fine di garantire la sicurezza europea-Conference on Security and Money Flows in the European Union*", organizzato dall'Unità di informazione Finanziaria per l'Italia, dalla Fondazione Bruno Kessler, BeSEC Boosting European Security Law and Policy e da Erasmus Programme of the European Union, Roma, 24—25 ottobre 2019, consultabile in www.discrimen.it del 2 dicembre 2019, p. 27.

[250] In questo senso SCOPINARO, *Acquisto e utilizzo illeciti di carta di credito via internet*, nota a Cass. Sez. I, 5-11-2002 n. 37115, in *Diritto penale e processo*, n. 6/2003, p. 735, la quale definisce analogia in *malam partem* il riconoscimento, operato con la pronuncia annotata, del delitto d'indebito utilizzo nell'impiego delle codici riferibili alla carta di credito.

[251] Si rinvia per l'analisi delle fattispecie nazionali sul punto al paragrafo III del cap. III.

[252] Sull'analisi critica di questa nozione e delle relative fattispecie penali applicabili si rinvia a GROTTO, *Regime giuridico del falso informatico e dubbi sulla funzione interpretativa dell`art. 491-bis c.p.*, in *Diritto dell'informazione e dell'informatica*, n. 4-5/2006, p. 589 ss.; CAUTERUCCIO, *I nuovi reati contro la fede pubblica: il falso in documento informatico pubblico o privato*, in *Rivista penale*, 10/2007, p. 965 ss.; PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, *cit.*, p. 701-704; SALCUNI, *Le falsità informatiche*, in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime*, *cit.*, p. 273 ss..

[253] Così la rubrica dell'art. 7 della direttiva UE/2019/713.

[254] L'art. 7 della direttiva UE/2019/ 713, mediante richiamo agli artt. 4 e 5, lett. a) e b), e all'art. 6, ammette l'incriminazione delle condotte "strumentali" alla contraffazione/ falsificazione, al furto/ottenimento illecito ed alla frode informatica comportante un trasferimento di denaro, di valore monetario o di valuta virtuale.

presto superate, sembra destinata, però, ad alimentare incertezze sia nell'individuazione di questi reati, sia nel coordinamento o possibile concorso con i delitti che già garantiscono un'analoga tutela anticipata.

Solo limitandosi ai reati informatici mediante i quali sarebbe conseguibile l'ottenimento illecito di uno strumento di pagamento immateriale, è da chiedersi se il regime diversificato individuato dal proposto art. 493 quater sia sempre applicabile quando si verifichi il predetto ottenimento, a discapito di altre previsioni astrattamente integrabili, come gli art. 615 quater[255] e 617 quinquies[256] c.p., che, già a una semplice lettura, delineano, però, delitti oggettivamente e soggettivamente non sovrapponibili[257].

Per essere più chiari, limitandosi in questa fase solo ad una breve comparazione con l'art. 615 quater c.p., questa fattispecie contempla, come oggetti materiali, anche, codici, parole chiavi o altri mezzi, indicazioni o istruzioni idonee all'accesso[258], l'art. 493 quater portato dallo schema del decreto legislativo in esame nulla, invece, prevede sul punto, nonostante sia riferibile alle chiavi private una valenza autenticativa analoga a quella dei menzionati oggetti[259]. Rispetto a queste ipotesi

---

[255] Si riporta di seguito il testo dell'art. 615 quater c.p.: "*Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164. La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1 e 2 del quarto comma dell'articolo 617 quater*".

[256] Si riporta di seguito il testo dell'art. 617 quinquies c.p.: "*Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte 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. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617 quater*".

[257] L'art. 615 quater c.p. individua un delitto di pericolo indiretto a dolo specifico di profitto, che si consuma nel momento in cui il soggetto agente acquisisce la disponibilità del codice di accesso ovvero nel momento in cui viene compiuto il primo atto di diffusione o si realizza la comunicazione o la consegna a terzi di tali mezzi, o di informazioni sul modo di eludere le barriere di protezione di un sistema informatico. L'art. 617 quinquies c.p. è, invece, reato di pericolo concreto a dolo generico, che si consuma nel momento in cui è installata apparecchiatura oggettivamente idonea a intercettare, impedire o interrompere delle comunicazioni informatiche o telematiche. Per l'analisi degli elementi costitutivi di entrambe le fattispecie si rinvia a C. PECORELLA, *sub art. 615 quater e sub art. 617 quinquies c.p.*, in DOLCINI-GATTA, *Codice penale commentato*, Tomo III, V ed., 2021, rispettivamente p. 2072 ss. e p. 2148 ss.

[258] Per SALVADORI, *I reati contro la riservatezza informatica*, in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime*, *cit.*, p. 697, per "*«codice» o «parola chiave» deve intendersi qualsiasi sequenza alfanumerica (o password) idonea a consentire a chi ne ha la disponibilità di accedere ad un sistema informatico protetto da misure di sicurezza. Mediante la locuzione «altri mezzi idonei», che si configura quale "clausola di chiusura" estremamente elastica, capace di ricomprendere anche gli strumenti tecnologici non ancora scoperti, il legislatore ha voluto sanzionare non solo i software multifunzionali o multiscopo che consentono di aggirare le misure di sicurezza poste a protezione di un sistema informatico e di accedere ai dati ed ai programmi in esso contenuti (c.d. hacking tools), ma anche qualsiasi dispositivo o mezzo fisico (ad es. una tessera magnetica), che permetta di introdursi in un sistema (…)Nella locuzione di chiusura «indicazioni o istruzioni idonee al predetto scopo» rientrano le informazioni che permettono di aggirare o eludere le misure di sicurezza poste a protezione di un sistema informatico*".

[259] In termini analoghi FLOR, *Financial cybercrime & Cryptocurrencies: le prospettive applicative del diritto penale vigente*, in GUARDIA DI FINANZA (a cura di), *Atti della Giornata di studi "Le criptovalute: funzionamento,*

prospettare l'operatività esclusiva del neo delitto di detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti genererebbe, quindi, un vuoto di tutela illogico ed inaccettabile. La differente struttura e portata valoriale di questo delitto indicato dallo schema del decreto è destinata, in generale, a creare frizioni, se si considera che qualsiasi ipotesi di ottenimento illecito presuppone l'apprensione delle predette chiavi, senza la quale non sarebbe possibile avere alcuna potere autorizzativo o di controllo sui trasferimenti di *virtual asset*.

Proprio per questa peculiarità, la questione è destinata a complicarsi con riferimento alla commissione del delitto di frode informatica, rispetto al quale sono già emerse difficoltà di coordinamento con l'indebito utilizzo ai sensi dell'art. 493 ter c.p.[260].

Queste difficoltà sembrano destinate ad acuirsi, potendo essere non semplice stabilire quando l'utilizzo della chiave privata illecitamente ottenuta possa effettivamente integrare l'uno o l'altro reato e se la predetta chiave sia, anche, qualificabile quale identità digitale ai fini della ricorrenza dell'aggravante del quarto comma dell'art. 640 ter c.p.[261].

---

regolamentazione, profili applicativi e principali riflessi per la polizia economico finanziaria", Verona, 28 maggio 2019, p. 60 ss..

[260] La giurisprudenza, pur concordando sull'individuazione-quale elemento differenziale che determinerebbe la ricorrenza della sola frode informatica- dell'utilizzazione fraudolenta del sistema informatico, appare divisa sui casi in cui essa sarebbe ricorrente: alcune pronunce ritengono sufficienti la mera digitazione dei codici in servizi on line, altri richiedono un *quid pluris*. Per un esame dei termini di questo contrasto si rinvia a LEO, *Sulla qualificazione dell'utilizzo abusivo nel circuito informatico dei codici concernenti carte di credito*, in *Diritto Penale e Processo*, 6/2013, p. 660 ss.. Come recente espressione del secondo orientamento indicato vedi Cass., sez. II, 1° luglio 2020, n. 21831 in *Diritto di internet*, 4/2020, con nota di GUERRA, D'ANELLO, p. 177 ss. Con questa pronuncia la Corte ha ribadito, il principio espresso in altri precedenti che "*in ipotesi di utilizzo di carte con banda magnetica falsificata, acquisizione illegittima dei codici segreti di accesso al sistema bancario, inserimento senza diritto nel sistema stesso, ordine di pagamento, con intervento sui dati contabili del sistema, ipotesi nelle quali rientra la fattispecie concreta oggetto del ricorso in esame, è ravvisabile solo il reato di frode informatica, in quanto l'elemento specializzante costituito dall'utilizzazione fraudolenta del sistema informatico costituisce presupposto assorbente rispetto alla generica indebita utilizzazione di una carta di credito, iscritta, come ratio, nel novero di misure destinate al controllo dei flussi finanziari, in funzione di prevenzione del riciclaggio*". In senso critico sull'atteggiamento ambivalente della Corte ed in generale per l'esclusione del concorso con operatività del solo delitto d'indebito utilizzo vedi FALDUTI, *Frode informatica e utilizzo indebito di carte di credito: variabili interpretative*, in *Giurisprudenza penale web*, 12/2017, p. 1 ss. ed in particolare p. 10 per cui "*dal punto di visto sistematico, inoltre, apparirebbe poco funzionale sottoporre ad una fattispecie con pena più grave e una procedibilità d'ufficio, le ipotesi di possesso, falsificazione, detenzione e cessione di carte di credito (tutte condotte realizzabili da remoto e senza materialità della carta), e al contempo, nel caso di utilizzo, ricomprendere tutto il paradigma fattuale appena richiamato nel novero di un generico "intervento senza diritto su dati", applicando l'art. 640 ter c.p. con una pena più bassa, e solo laddove sia soddisfatta la condizione di procedibilità. Per le ragioni sopraesposte, la condotta di chi, ottenuti i dati relativi ad una carta di credito, indebitamente li utilizzi, non essendone titolare, come metodo di pagamento al fine di trarne profitto, appare meglio adattarsi all'ipotesi di reato di cui all'art. 55 d. lgs. 231/2007*".

[261] Riservando al paragrafo 3.3. la trattazione del tema, si rappresenta che sulla base della relazione dell'ufficio del massimario della Corte di Cassazione curata da PISTORELLI, *Prime note sulla legge di conversione, con modificazioni, del d.l. n. 93 del 2013, in materia tra l'altro di "violenza di genere" e di reati che coinvolgano minori*, in www.dirittopenalecontemporaneo.it, p. 7, l'identità digitale è definita come "*l'insieme delle informazioni e delle risorse concesse da un sistema informatico ad un particolare utilizzatore del suddetto sotto un processo di identificazione, che consiste (per come definito invece dall'art. 1 lett. u ter del d.lgs. 7 marzo 2005 n. 82) per l'appunto nella validazione*

Con riferimento alla frode informatica lo schema del decreto legislativo in esame non dà risposta a nessuno di questi interrogativi, anzi, partendo dalla considerazione che la fattispecie nazionale punisca, già, le condotte oggetto degli obblighi d'incriminazione, contempla l'introduzione, al secondo comma dell'art. 640 ter c.p., solo della circostanza aggravante della "produzione" di un trasferimento di denaro o valore monetario o di valuta virtuale[262]. Un intervento di questo tipo è stato giustificato dal fine dichiarato di riparametrarne il regime sanzionatorio su quelle fissato dall'art. 493 ter c.p. e conformarsi al giudizio di maggior disvalore previsto per queste ipotesi dall'art. 9, par. 4, della direttiva UE/2019/713[263].

Per questa fattispecie aggravata e per le altre due, qui sinteticamente esaminate, lo schema del decreto legislativo contempla, poi, l'introduzione anche della responsabilità amministrativa dipendente da reato delle persone giuridiche, mediante inserimento nel d.lgs. 231/2001 dell'art. 25 octies.1, rubricato "*illeciti in materia di mezzi di pagamento diversi dai contati*".

Con questo articolo, che andrebbe inserito subito dopo quella relativa alla "*ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio*", si intende fissare relativamente al delitto di cui all'art. 493-ter c.p.- da cui dipenda la responsabilità dell'ente-il medesimo trattamento sanzionatorio adottato dall'art. 25 *bis* del d.lgs. 231/01 per la falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate[264], mentre si stabilisce per l'ipotesi di frode informatica aggravata e per i delitti di cui all'art. 493 quater c.p. la sanzione pecuniaria in misura corrispondente a quella fissata per la frode informatica commessa in danno dello Stato o di altro ente pubblico dall'art. 24 d.lgs. 231/2001[265].

---

dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche alfine di garantire la sicurezza dell'accesso".

[262] Si riporta di seguito il testo del secondo comma dell'art. 640 ter c.p. come coordinato con le modifiche previste dallo schema di decreto legislativo: "*la pena è della reclusione da uno a cinque anni e della multa da trecentonove euro a millecinquecentoquarantanove euro se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, se produce un trasferimento di denaro, di valore monetario o di valuta virtuale, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema*".

[263] In questo senso la relazione illustrativa, *cit.*, p. 4.

[264] Si tratta della sanzione pecuniaria da trecento ad ottocento quote, fissando l'art. 25 bis del d.lgs. n. 231/01 per la responsabilità amministrativa dipendente dagli altri reati in materia di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento sanzioni più lievi. Sull'origine e l'analisi del contenuto di questa disposizione vedi PICCINNI, *I delitti contro la fede pubblica e la responsabilità amministrativa delle persone giuridiche e delle società alla luce dell'articolo 25 bis del d.lgs.231/2001*, in *Interventi-Rivista 231*, gennaio 2016.

[265] Si tratta della sanziona pecuniaria di 500 quote. Sul recente ampliamento del novero dei reati previsti dall'art. 24 in forza dell'attuazione, mediante il d.lgs. n. 75/2020, della direttiva UE/2017/1371, cd. PIF, recante norme per la lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale, vedi CORSARO, *Il recepimento della Direttiva PIF e le novità in materia di reati contro la pubblica amministrazione e reati tributari. L'ulteriore ampliamento dei reati presupposto per la responsabilità degli enti*, in www.giurisprudenzapenale.com del 20 luglio 2020.

Questa disposizione, che solleva perplessità a partire dalla formulazione letterale certamente ambigua nella declinazione al singolare del ventaglio di fattispecie[266] dell'art. 493 ter c.p., non appare adeguatamente coordinata con i livelli sanzionatori previsti per la responsabilità amministrativa dipendente dalla commissione dei delitti di cui agli artt. 615 quater e 615 quinqies c.p.[267] .

Se si guarda, poi, alla previsione del delitto di frode informatica solo nella versione aggravata da introdurre, la percezione in generale che si ha è quella di un'occasione mancata: l'attuazione della direttiva poteva essere sfruttata per l'introduzione di questo delitto fra i reati presupposti anche nell'ipotesi base[268].

Da questa prima analisi risulta, ad avviso di chi scrive, come ai fini del recepimento della direttiva UE/2019/713 sia stata ritenuta sufficiente l'estensione alle frodi e falsificazioni degli strumenti di pagamento immateriali delle scelte e del trattamento già previsto per quelli materiali, senza operare, però, gli opportuni adattamenti richiesti, né tantomeno adottare quelle misure necessarie di raccordo con i delitti informatici, patrimoniali e non, certamente integrabili con riferimento a questi strumenti.

Che il legislatore europeo abbia un approccio casistico è per certi versi ammissibile se si tiene conto del carattere settoriale delle direttive penali, ma questo stesso approccio non è, invece, tollerabile da parte del legislatore nazionale, che avrebbe dovuto operare quella revisione organica del sistema imposta dal recepimento sostanziale delle scelte di politica criminale sovranazionale.

Riservando al proseguo l'esame delle implicazioni che potrebbero derivare dall'approvazione definitiva del schema del decreto legislativo in esame, particolarmente rilevante, per la verifica delle tecniche d'incriminazione "compatibili" con la digitalizzazione del sistema economico, è l'approfondimento, che si intende operare nei paragrafi successivi, di quel giudizio, che sembra riferibile anche al legislatore nazionale, di estraneità delle modalità acquisitive degli strumenti di pagamento immateriali dalle forme di manifestazione dei tradizionali delitti contro il patrimonio, compresa l'appropriazione indebita a cui si riferisce la terminologia sovranazionale.

---

[266] Per una migliore comprensione si riporta di seguito il testo dell'art. 25 octies.1: "*In relazione alla commissione degli illeciti previsti dal codice penale in materia di mezzi di pagamento diversi dal contante, si applicano all'ente le seguenti sanzioni pecuniarie: a) per il delitto di cui all'art. 493.ter la sanzione pecuniaria da 300 a 800 quote; b) per i delitti di cui agli articoli 493-quater e 640-ter, secondo comma, la sanzione pecuniaria sino a 500 quote. Nei casi di condanna per uno dei delitti di cui al comma 1 si applicano all'ente le sanzioni interdittive previste dall'art. 9, comma 2*".

[267] L'art. 24 bis del d.lgs. n. 231/01 fissa la sanziona pecuniaria sino a trecento quote. Per una disamina del contenuto di questa disposizione si rinvia a SANTORIELLO, *I reati informatici dopo le modifiche apportate dalla legge 48/2008 e la responsabilità degli enti*, in *La Responsabilità amministrativa delle società e degli enti*, 1/2011, p. 211 ss.

[268] In questo senso BELTRANI, *Reati informatici e d.lgs. 231/2001 alla luce della legge di attuazione della Convenzione di Budapest*, in *La Responsabilità amministrativa delle società e degli enti*, 4/2008, p. 21.

Operata questa verifica, in quella visione più ampia, che vuole essere qui seguita, d'individuazione delle coordinate della tutela penale degli scambi digitali, verranno verificate le implicazioni di tipo, anche, valoriali, emergendo già in questa fase la connessione con beni ulteriori.

Altro ambito conseguente di analisi sarà, allora, verificare quale possa essere rispetto a questo assetto il ruolo della sicurezza informatica: se quella dimensione "interferenziale" che è stata colta nell'analisi dell'impronta assiologica dell'intervento sovranazionale sia semplicemente declinabile in termini di plurioffensività o se assuma una valenza diversa, di sintesi delle commistioni "valoriali" in chiave dogmatica nuova.

2. *il raffronto con le fattispecie nazionali*

La verifica del giudizio di estraneità, sopra menzionato, delle modalità acquisitive degli strumenti di pagamento immateriali dalle forme di manifestazione dei tradizionali delitti contro il patrimonio richiede, a monte, la verifica della compatibilità di questi delitti con il "nuovo" oggetto o mezzo costituito dai dati informatici.

A tal fine bisogna considerare che alcuni dei tradizionali reati contro il patrimonio del Codice Rocco possono anche realizzarsi quali reati cibernetici in senso ampio[269], in quanto si può ricondurre all'astratta tipizzazione espressa dalle disposizioni in esame anche la commissione digitale.

Come già accennato[270], esemplificativo in questo senso è il delitto truffa[271]. Ai fini della sua sussistenza, ciò che rileva è il "*vincolo di strumentalità*" che "*rende l'artifizio-raggiro il mezzo necessario per tipizzare l'offesa al patrimonio della vittima*"[272]: rispetto a questo contenuto modale identificativo è indifferente il carattere digitale dello strumento prescelto.

Allo stesso modo non si può dubitare della riconduzione all'art. 648 c.p. del c.d. *cyberlaundering*[273]: "*l'elastica clausola di chiusura finale*"- *compiere altre operazioni*- "*non richiede alcuna specifica modalità*

[269] Sulla definizione di reato cibernetico vedi nota 70 del cap. I.

[270] Vedi in proposito il paragrafo 4 del capitolo II.

[271] In questo senso FLOR, *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di internet*, *cit.*, p. 4 nota 12, con riguardo alla truffa che sia commessa, ad esempio, mediante l'invio di email ingannevoli che inducono in errore il destinatario, determinandolo ad effettuare un atto di disposizione patrimoniale su conti correnti online; in generale per l'Autore si tratta di ipotesi di reato che, pur non presentando espressamente elementi tipici caratterizzati dalla tecnologia, sia riferibile anche a fatti commessi tramite la tecnologia, la rete o nel cyberspace.

[272] FALCINELLI, *Memento sulla tipicità penale dell'atto di disposizione del patrimonio*, in *Archivio penale*, 2/2012, p. 13.

[273] PICOTTI, *Profili penali del cyberlaundering: le nuove tecniche di riciclaggio*, *cit.*, p. 591, definisce il *cyberlaundering* come "*fenomeno complesso che comprende l'insieme di tutte le attività illecite finalizzate a ripulire (letteralmente: lavare) non solo il denaro (moneylaundering), ma più in generale i capitali, i beni, i valori o le altre utilità di provenienza delittuosa, ricorrendo a sistemi o mezzi elettronici o, meglio, "cibernetici", resi possibili dalle TIC, che coinvolgono oggi soprattutto la rete*".

tecnica, ne´ alcun univoco risultato finale, della condotta punibile, bastandone l'idoneità ad "ostacolare" l'identificazione della provenienza, sia oggettiva, che soggettiva, di valori ed "utilità", senza che occorra un'assoluta impossibilita`, ne´ che vi sia un vincolo definitorio alla materialità fisica degli oggetti della condotta stessa, estesi ben oltre l'ambito tradizionale del "denaro" o della moneta tradizionalmente intesa"[274].

La predetta fattispecie identifica, in particolare, quale oggetto materiale su cui ricade l'azione ostativa, oltre al denaro, "*i beni o altre utilità*"[275]: espressione questa che gli attribuisce una potenzialità inclusiva massima riferibile a "*qualsiasi entità economicamente apprezzabile, materiale o immateriale, mobile o immobile, compresi documenti o titoli comprovanti il diritto di proprietà o altri diritti*"[276].

Discorso diverso vale, invece, per la ricettazione e, a monte, per il delitto di furto che, facendo riferimento rispettivamente al denaro o a "cose" provenienti da delitto[277] e alla "cosa mobile altrui"[278], sono ritenuti applicabili con riguardo ai beni immateriali solo relativamente ai supporti che li incorporino[279].

---

[274] Testualmente PICOTTI, *op. cit.*, p. 608.

[275] DELL'OSSO, *Riciclaggio di proventi illeciti e sistema penale,* Torino, 2017, p. 112, per cui "*sembra corretto immaginare che la scelta del Legislatore del 1990 sia stata proprio nella direzione di prevenire discussioni sulla sorte di specifiche forme di ricchezza, sancendo in via preliminare la riciclabilità di ogni tipologia di valore*".

[276] Cfr. Cass. pen. Sez. II, 17.01.2012, n. 6061 secondo cui "*Ciò è desumibile sia dall'inequivoco tenore letterale della norma, che dalla considerazione dell'excursus normativo che ha portato all'attuale formulazione. Rispetto al testo originario, introdotto dalla L. n. 191 del 1978, si è provveduto già con l'art. 23 L. n. 55 del 1990 a sostituire la generica espressione altri valori con quella più puntuale altri beni o altre utilità con l'evidente proposito di eliminare incertezze applicative e di evitare, soprattutto, spazi d'impunità in relazione a quelle categorie di beni, diversi dal denaro, che si poteva dubitare che rientrassero tra i valori. Anche un veicolo di provenienza delittuosa può perciò costituire l'oggetto materiale di una condotta di riciclaggio*". In dottrina nel senso che l'oggetto di riciclaggio sia identificabile, alla luce della formulazione normativa unitariamente letta, con un contenuto economico in termini di liquidità e spendibilità vedi DELL'ANNO, *Il delitto di riciclaggio: contrasto tra la previsione normativa e le applicazioni giurisprudenziali*, in *Cass. Pen.*, 11/2003, p. 3436; DELL'OSSO, *Riciclaggio di proventi illeciti e sistema penale, cit.*, p. 113.

[277] Nella manualistica F. MANTOVANI, *Diritto penale, parte speciale*, cit., p. 283 considera oggetto della ricettazione solo le cose sia mobili sia immobili, escludendo sia le utilità che i beni immateriali. In senso parzialmente difforme relativamente all'inclusione dei beni immobili FIANDACA, MUSCO, *Diritto penale. Parte speciale*, *cit.*, p. 247. In dottrina per la tesi estensiva Cfr. PECORELLA, voce *Ricettazione*, in *NN.D.I.,* XV, 1968, p. 943; REINOTTI, voce *Ricettazione e riciclaggio*, in *Enc. dir.,* XL, 1989, p. 469; LONGOBARDO, *Ricettazione*, in FIORE (a cura di), *I reati contro il patrimonio*, Utet, 2010 p. 790.

[278] Nel senso di una nozione di cosa in termini fisici-materiali, da un lato più ristretta di quella civilistica, non comprendendo beni immateriali e diritti, dall'altra più ampia, perché includente anche le cose mobilizzate, vedi nella manualistica ANTOLISEI, *Manuale di diritto penale. Parte speciale*, *cit.*, p. 382; in dottrina si rinvia a Cfr. PECORELLA, voce *Furto*, *cit.* , p. 334; più recentemente RESTA, *Il delitto di furto. Profili sostanziali e strategie processuali alla luce delle più recenti evoluzioni normative,* Cedam, 2010, p. 49, evidenzia che "*ai fini dell'individuazione della categoria delle cose la cui sottrazione rilevi ai sensi dell'art. 624 c.p., è importante considerare se l'impossessamento del bene, da parte del soggetto attivo, determini o meno la perdita di disponibilità di esso per la persona offesa, ravvisandosi gli estremi del furto soltanto nella prima ipotesi. In tal senso, si è affermato in giurisprudenza che è da escludere la configurabilità del reato di furto nel caso di semplice copiatura non autorizzata di "files" contenuti in un supporto informatico altrui, non comportando tale attività la perdita del possesso della "res" da parte del legittimo detentore (Cass., IV, sent. n. 3449 del 29.1.2004 (ud. del 13.11.2003), rv 229785)*".

[279] Con riferimento alla ricettazione si rinvia a GALANTE, *Ricettazione: l'interpretazione giurisprudenziale di una fattispecie problematica*, in *Diritto penale e processo*, 11/2017, n. 11, p. 1530-1531; per un'applicazione

Questo orientamento è fondato sulla concezione in termini tangibili corporali della nozione di "cosa" oggetto materiale di questi reati[280].

Anche in considerazione della difficoltà di coniugare una concezione penalistica di cosa con quella civilistica[281], ad avviso di chi scrive, la sua determinazione è fortemente influenzata dal punto di vista dell'osservatore.

Con riferimento al diritto penale non esiste una definizione normativa di "cosa". L'unica previsione espressa, la quale appare, però, priva di valenza generale[282], riguarda il delitto di furto e, cioè, l'assimilazione alla cosa mobile, ai sensi del secondo comma dell'art. 624 c.p., dell'energia elettrica e di ogni altra energia che abbia valore economico[283].

Deriva da quanto sopra che la sua identificazione o meno con un'oggettività fisico-naturalistica è questione dipendente dalla specificità della fattispecie incriminata[284]. Di conseguenza, anche

giurisprudenziale si rinvia a Tribunale di Milano, 25 settembre 2013 - Est. Calabi, con nota di GATTA-TURCHETTI-VARRASSO, in *Il corriere del merito,* n. 12/2013, p. 1178 ss.; di recente circa la ricettazione di cd rom contenente telefonate illecitamente registrate anche Cass., Sez. II, sent. 7 giugno (dep. 19 settembre) 2019, n. 38277, con nota di ZUFFADA, *Giornalismo d'inchiesta e diritto penale: la Corte di cassazione apre le porte alla configurabilità della scriminante del diritto di cronaca rispetto al reato di ricettazione commesso dal giornalista*, in www.sistemapenale.it del 19 marzo 2020.

[280] F. MANTOVANI, *Umanità e razionalità nel diritto penale*, Cedam, 2008, p. 696, chiarisce come "*Ai fini dei reati patrimoniali assurge a cosa l'entità materiale su cui i beni immateriali (diritto di credito, idee, opera del pensiero, informazioni, programmi) vengono trasfusi (carta riproducente l'assegno, l'invenzione, la composizione musicale; dischetti per la registrazione dei programmi dei calcolatori elettronici; ecc.). Incorporando il bene immateriale, tali entità materiali acquisiscono il valore di questo, diventando cose idonee a soddisfare quei particolari bisogni umani (17). Pertanto costituisce furto la sottrazione del supporto magnetico, su cui è fissato il programma del calcolatore elettronico, e non anche la sottrazione dei dati senza l'asportazione di detto supporto (es.: mediante ascolto, riproduzione, intercettazione)*".

[281] In generale sul modo d'intendere i concetti di matrice civilistica, come appunto quello di cosa mobile o ancora di possesso o detenzione, richiamati dalle fattispecie penale vedi FIANDACA, MUSCO, *Diritto penale. Parte speciale*, *cit*., p. 22 che ritiene che non si possa in generale optare o per la tesi pancivilistica o per quella autonomistica, trattandosi di un tipico problema di interpretazione che va risolto caso per caso, e cioè in rapporto alle diverse figure di reato e alle rispettive finalità di tutela.

[282] In questi termini in senso critico sull'operatività di questa equiparazione anche al concetto di cosa di cui alla contravvenzione punita dall'art. 674 c.p. vedi GIZZI, *Inquinamento elettromagnetico e responsabilità penale: la Cassazione sul caso Radio vaticana*, in www.sistemapenale.it del 6 luglio 2011, p. 4, per cui "*La diversa soluzione – secondo cui in tutte le norme penali in cui figura la parola cosa trova applicazione la norma definitoria di cui all'art. 624 c.p., con la conseguenza che tale parola comprende sempre, oltre alle res corporales, anche le energie naturali – si fonda sull'erroneo presupposto della costanza terminologica nel linguaggio legislativo, per cui il legislatore impiega ciascun termine sempre con lo stesso significato, indipendentemente dal contesto linguistico e normativo in cui è collocato*". Nella stessa direzione anche TUZET, *La storia infinita ancora su analogia e interpretazione estensiva*, in *Criminalia*, 2011, p. 517.

[283] FIANDACA-MUSCO, *op. cit*., p. 66 evidenzia che per energia oggetto di furto si intende quelle che possono essere captate e utilizzate dall'uomo con profitto proprio e danno altrui, risultano di conseguenza escluse le energie umane e animali. Circa le questioni sorte in ordine alla sottrazione di energie concesse mediante contatore v. ARATO, *Furto di energia elettrica*, in *Diritto penale e processo*, 3/2010, p. 316 ss..

[284] In questo senso con riferimento al furto RESTA, *Il delitto di furto. Profili sostanziali e strategie processuali alla luce delle più recenti evoluzioni normative, cit.*, p. 45, secondo cui "*la funzione peculiare che il concetto di 'cosa mobile altrui' assolve nell'economia della fattispecie in esame, induce ad interpretare tale nozione non già sulla base di un rigido parallelismo con l'accezione fornitane dal codice civile (segnatamente agli artt. 812 ss..) ma alla luce della ratio e delle*

l'inclusione nel concetto di "cosa mobile" penalmente rilevante delle valute virtuali ed in generale dei dati informatici dipende dal singolo comportamento lesivo tipizzato dal reato, nella sintesi di tutti i suoi elementi costitutivi in reciproca interdipendenza definitoria, da cui è possibile estrapolare il fatto tipico, "*la specifica (modalità di) lesione dell'interesse giuridico protetto (bene giuridico)*"[285].

2.1 Al cospetto del delitto di furto

Iniziando dal delitto di furto, emerge come questo delitto sia incentrato su un rapporto di appartenenza a carattere reale[286].

L'art. 624 c.p., quale tipica fattispecie di aggressione unilaterale[287] in contrapposizione alla truffa, costituente il modello dei reati di cooperazione artificiosa con la vittima[288], incrimina con la reclusione da 6 mesi a tre anni e con la multa da 154 euro a 516 euro la condotta d'impossessamento della cosa mobile altrui mediante sottrazione da chi la detiene, al fine di trarne profitto per sé o per altri. Sulla base di questo formulazione è stata considerata suscettibile di furto solo quella entità "*che può essere materialmente spostata dalla sfera patrimoniale altrui alla propria*"[289].

esigenze di tutela sottese alla norma di cui all'art. 624 c.p., privilegiando dunque il criterio della suscettibilità di apprensione e sottrazione della cosa".

[285] Testualmente PICOTTI, *op. cit*, p. 536.

[286] Nel senso che oggetto del furto possa essere una cosa mobile materiale, definita spazialmente e dotata di esistenza autonoma, nonché le energie di cui al comma 2 dell'art. 624 c.p. in quanto suscettibili di sottrazione e godimento, in sintesi FORMICA, *I delitti di furto,* in VIGANÒ, PIERGALLINI (a cura di), *Reati contro la persona e contro il patrimonio*, p. 394-396.

[287] PEDRAZZI, *Inganno ed errore nei delitti contro il patrimonio*, *cit*., p. 41. Oltre al furto appartengono a questa categoria ampia anche la rapina, i danneggiamenti e l'appropriazione indebita, quali reati unificati da una nota costante: "*l'arbitrio unilaterale con cui il reo invade la sfera altrui*".

[288] PEDRAZZI, *Inganno ed errore nei delitti contro il patrimonio*, *cit*., p. 42, si tratta del gruppo di reati definiti di cooperazione artificiosa, in cui, in realtà, gli interessi dei soggetti-parti sono in realtà collidenti. All'interno di questo gruppo il Grande Maestro individua un'ulteriore categoria costituita da quelle fattispecie il cui il reo sfrutta la condizione di debolezza del soggetto passivo per ottenerne la collaborazione, come nel reato di circonvenzione d'incapace. Sulla preferenza per questa suddivisione, ancorché con ulteriori sotto classificazioni, rispetto a quella codicistica incentrata sulla violenza o frode cfr. MOCCIA, *Tutela penale del patrimonio e principi costituzionali*, *cit*., p. 125 ss.; *Contra* MARINI, *delitti contro il patrimonio*, *cit*., p. 33-34, che intende la violenza e la frode rispettivamente come "*mancanza di consenso*" e "*presenza di un consenso partecipativo non viziato da violenza e minaccia lesive della libertà di motivazione all'operare*".

[289] F. MANTOVANI, *Diritto penale, parte speciale*, cit., p. 28.

Le relative condotte, che hanno come presupposto la detenzione in capo al soggetto poi spossessato[290], sono, infatti, costituite dalla sottrazione, da un lato, e dall'impossessamento, dall'altro, secondo il modello dell'"*appropriazione mediante espropriazione*"[291].

Secondo autorevole dottrina alla connessione teleologica, sussistente tra il fine di profitto[292] che deve essere tratto dalla cosa e la condotta di sottrazione, corrisponde, sul piano oggettivo, uno spostamento patrimoniale da intendersi come sostituzione "*del soggetto passivo da parte dell'agente, nel potere di fatto di disporre e di goderne esclusivamente (cd. usurpazione unilaterale della signoria di fatto)*"[293].

La sottrazione e l'impossessamento, le quali costituiscono secondo la dottrina condotte autonome e distinte[294], sono senza dubbio connesse, nel senso che la privazione del controllo materiale sulla cosa è presupposto necessario del trasferimento in capo ad altro soggetto, con conseguenze in termini di perfezionamento e consumazione del reato[295].

---

[290] PECORELLA, voce *Furto*, *cit.*, p. 360, per cui la detenzione "*designa l'incidenza immediata dell'azione tipica, ed è anzi un complemento necessario del concetto di sottrazione: non si può sottrarre, è logico, se non la cosa su cui altri abbiano un potere di fatto*". Per un'analisi dottrinale e giurisprudenziale di questo potere di fatto in rapporto alla nozione di possesso che connota il delitto di appropriazione vedi LA MACCHIA, *Detenzione e possesso nel furto e nell'appropriazione indebita*, in *Cassazione penale*, 2/1982, p. 235 ss.; POERIO, *Possesso*, in *Studium iuris*, n. 12/2001, p. 1546 ss.; TAMBURRO, *Il bene giuridico protetto dal reato di furto: una questione anche di 'possesso'*, in *Rivista penale*, 6/2014, p. 551 ss..

[291] Così PICOTTI, *op. cit.*, p. 228; sulle origine e caratteristiche di questo modello che si deve alla dottrina tedesca si rinvia, anche, a p. 223-224 e note 56-58. L'Autore richiama, in particolare, la tesi di JAKOBS, il quale riconosce come l'appropriazione e l'espropriazione siano momenti distinti, che insieme, però, connotano il delitto di furto, dovendosi attribuire alla finalità appropriativa la funzione di determinare "*la specifica «modalità di lesione» del bene, piuttosto che un'anticipazione di questa*".

[292] Sulla ricostruzione giurisprudenza del contenuto del fine di profitto nel contesto in generale dei reati contro il patrimonio e specificatamene in senso critico sulla tesi maggioritaria che lo concepisce in termini ampi, includendo qualunque piacere o soddisfazione che il soggetto agente si procuri attraverso l'azione criminosa, si rinvia a SICCARDI, *Il "fine di profitto" nei delitti contro il patrimonio*, in *Diritto penale e processo*, n. 3/2016, p. 358 ss.. *Contra* la considerazione di questo fine quale dolo specifico CARMONA, *Tutela penale del patrimonio individuale e collettivo*, *cit.*, p. 201-207, che ritiene che il furto sia delitto a "*dolo generico esplicitato*".

[293] PICOTTI, *op. ult. cit.*, p. 228, che chiarisce anche come "*benché formulato, a livello di tipo normativo, come dato soggettivo ed ulteriore rispetto alla condotta, il fine specifico puntualizza, così, l'oggettivo significato di appropriazione, che deve avere l'impossessamento materiale della cosa, per realizzare il reato*".

[294] In questo senso ANTOLISEI, *Manuale di diritto penale. Parte speciale*, cit., p. 413, che li considera anche non logicamente correlati e ritiene che il furto si perfezioni con l'impossessamento creativo di un nuovo possesso. *Contra* PECORELLA, voce *Furto*, *cit.*, p. 356.

[295] FIANDACA-MUSCO, *Diritto penale. Parte speciale*, *cit.*, p. 62, per cui finché alla sottrazione non segue l'acquisizione di un nuovo possesso si avrà solo un furto tentato; in senso analogo anche MARINI, *delitti contro il patrimonio*, *cit.*, p. 117, il quale considera, però, la sottrazione elemento eventuale che concorre, se sussistente, a meglio individuare l'impossessamento. Per un esame giurisprudenziale di alcune ipotesi che hanno generato contrasti sull'individuazione del momento di consumazione del furto si rinvia a MANCINI, *Il furto nei supermercati: la linea di confine tra tentativo e consumazione*, in *Cassazione penale*, n. 3/2000, p. 608 ss.; AMOROSO, *La sorte dei furti di generi di prima necessità all'interno dei supermercati all'indomani della pronuncia delle Sezioni Unite n. 52117/2014 e dell'introduzione dell'art. 131-bis nel codice penale*, nota a Cass. pen., S.U., 17.07.2014, n.52117, in *Cassazione penale*, n. 6/2015, p. 2168 ss.; CISLAGHI, *Ancora sul momento consumativo del delitto di furto*, in www.sistemapenale.it del 17 luglio 2015; CORBETTA, *Ladro che occulti la refurtiva: furto tentato o consumato?*, in *Diritto penale e processo*, n. 5/2018, p. 626 ss..

Con riferimento alle entità digitali, la loro attitudine ad essere trattate, riprodotte o tramesse, indipendentemente dall'incorporazione in un supporto fisico, da più soggetti contemporaneamente le rende insuscettibili di apprensione mediante privazione della loro disponibilità[296]: per essere più chiari, il momento acquisitivo non deriva né passa necessariamente dalla perdita del possesso da parte della vittima[297]; ne consegue pertanto che, come autorevolmente rappresentato, "*un «furto» senza sottrazione non è un furto*"[298].

Nonostante quanto sopra, parte della dottrina ha considerato l'inoperatività del furto rispetto alle entità digitali come un vuoto di tutela da colmare *de iure condendo*[299] o addirittura già *de iure condito*, in forza della praticabilità di un'interpretazione estensiva al passo con l'evoluzione tecnologica[300].

Nello specifico, la predetta interpretazione estensiva consentirebbe, da un lato, una concezione di "cosa" conforme alla realtà digitale[301], dall'altra, potrebbe essere fondata su un argomento normativo espresso, costituito dalla previsione, come circostanza aggravante della frode informatica, del "furto o indebito utilizzo di identità digitale"[302].

---

[296] In questo senso PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, *cit.*, p. 711, per cui "*i "dati", al pari delle "informazioni" e dei "programmi", per la loro immaterialità non possono giuridicamente essere oggetto di "possesso", come lo sono le "cose""*. In senso analogo si è espressa la giurisprudenza, tra le tante Cass. pen., Sez. II, 14.09.2006, n. 30663, con nota di SCOPINARO, *Furto di dati e frode informatica*, in *Diritto penale e processo*, 3/2007, p. 363 ss., che individua nel fatto di riproduzione non autorizzata, in copia, di programmi aziendali e notizie riservate- compiuto mediante accesso al sistema operativo aziendale- il concorso fra i delitti di accesso abusivo ad un sistema informatico o telematico e di frode informatica; Cass. pen., Sez. IV, 21.12.2010, n. 44840, con nota di CORBETTA, *Furto di files*, in *Diritto penale e processo*, 2/2011, p. 160 ss., per cui "*Non sussiste il delitto di furto nel caso di copiatura non autorizzata di files contenuti in un supporto informatico altrui, non comportando tale attività la perdita del possesso della res da parte del legittimo detentore*"; Cass. pen. , 29.05.2019, n.26604, sez. II, in *Diritto & Giustizia*, n. 111/2019, p. 9; Cass. pen. Sez. I, 17 giugno 2019, n. 26625 consultabile alla banca dati on line *www.pluris-cedam.utetgiuridica.it*.

[297] Cfr. PICOTTI, *Studi di diritto penale dell'informatica*, Tipogr. Godo, Verona, 1992, p. 112, chiarisce come diversamente dall'energia, dati e programmi informatici sono "*suscettibili di riproduzione, trasmissione, elaborazione e quindi poi autonomo trattamento e godimento ulteriori senza che debba farsene oggettivamente perdere la disponibilità e fruibilità anche al legittimo titolare*".

[298] PECORELLA, voce *Furto*, *cit.*, p. 357.

[299] In questo senso VINCIGUERRA, *Due anni alla commissione ministeriale per la riforma del codice penale. Un consuntivo*, in *Dir. pen. XXI secolo*, 2004, 103 ss..

[300] Sul tema generale del rapporto tra sviluppo tecnologico ed interpretazioni ammissibile nel diritto penale si rinvia a LEUCCI, *Appunti sul difficile rapporto tra linguaggio, diritto penale e tecnologia*, in *Informatica e diritto*, 2013, fasc. 2, p. 151 ss..

[301] SOLA, *Tutela dei beni immateriali e reati contro il patrimonio: alcune osservazioni*, in *Ind. Pen.*, 1990, p. 789-790, secondo cui, alla luce dello sviluppo economico e dei rapporti giuridici, "*ciò che conta per l'appartenenza alla categoria dei beni è la presenza di due requisiti fondamentali: la riconducibilità all'autore e, soprattutto, il valore commerciale che essa esprime*".

[302] FALCINELLI, *Tempi moderni e cultura digitale: il valore patrimoniale dell'identità umana "on line"*, in *Ind. pen.*, 3/2015, p. 326. L'Autrice ritiene che con l'introduzione di questa aggravante la frode informatica costituirebbe un'ipotesi di reato complesso in cui, dal lato "*del "fatto risultato", sta l'atto di disposizione patrimoniale realizzato dalla vittima dell'inganno consistito nel rappresentare una situazione inveritiera (di spettanza dell'identità digitale utilizzata) al sistema informatico/telematico, dal lato del "fatto strumento" vi è il segno dell'altruità della cosa/identità digitale*".

Tenendo conto della natura della cosa, quale *genus* rispetto alla *species* bene individuata dall'art. 810 c.c.[303], ricomprendente sia le cose materiali sia quelle immateriali, si è ritenuto che l'inclusione di queste ultime nel concetto penalistico di "cosa mobile" non sarebbe contraria al principio di legalità, costituendo la mera estrapolazione di uno dei possibili significati abbracciati dalla nozione di sintesi[304].

Sulla base, invece, della previsione della segnalata circostanza aggravante, di cui all'art. 640 ter, terzo comma, c.p., costituita dal "furto o indebito utilizzo dell'identità digitale" si è sostenuto che sarebbe stato, da un lato, operato il riconoscimento dell'identità digitale come bene mobile altrui[305], e, dall'altro, codificato il dualismo dell'illecita apprensione dei dati identitari e del loro utilizzo abusivo. In questo modo si sarebbe, così, meglio normativizzata la sostanza delle moderne forme di aggressione patrimoniale rispetto alla "*separazione notoriamente invalsa nell'indagine tra unauthorized access (accesso non autorizzato a sistemi altrui / possesso non autorizzato di dati altrui) e unauthorized use (uso non autorizzato di dati altrui lecitamente posseduti)*"[306].

Le tesi esaminate non possono essere condivise per differenti ragioni, che attengono sia al rispetto dei limiti dell'esegetica ammessa nel diritto penale[307], sia alla separazione esistente tra il piano assiologico e quello della tipicità codificata[308].

---

[303] SOLA, *Tutela dei beni immateriali e reati contro il patrimonio: alcune osservazioni*, cit., p. 791. L'Autore ritiene che poiché la *species* deve avere tutte le caratteristiche del *genus* e nella *species* bene sono ricomprese anche le entità immateriali suscettibili di valutazione economica, la cosa penalmente rilevante, quale *genus*, può essere, pertanto, indifferentemente materiale o immateriale.

[304] SOLA, *op. cit.* p. 793.

[305] FALCINELLI, *Tempi moderni e cultura digitale: il valore patrimoniale dell'identità umana "on line"*, *cit.*, p. 318.

[306] FALCINELLI, *op. cit.*, p. 327.

[307] Senza alcuna pretesa di esaustività, per l'analisi di questi limiti in rapporto al divieto di analogia a si rinvia PULITANÒ, *Principio di legalità ed interpretazione della legge penale*, in COCCO (a cura di), *Interpretazione e precedente giudiziale in diritto penale*, Padova, 2005, p. 27ss; DI GIOVINE, *L'interpretazione nel diritto penale tra creatività e vincolo alla legge*, Milano, 2006; ID., *L'attuale, il frainteso e il superato dell'ermeneutica penale nel contesto italiano*, in *Ars Interpretandi*, 2-2020, p. 67 ss.; GAETA, *L'illusione della monade chiusa: primato del caso e crisi della tipicità penale*, in *Ars interpretandi* 1/2019, p. 111 ss.; SERRA, *Interpretazione estensiva vs divieto di analogia: una problematica tradizionale in una recente (e criticabile) pronuncia della Corte di Cassazione*, in *Diritto penale contemporaneo*, 6/2018, p. 137 ss.; DE ROSA, *Il punto sull'analogia nel diritto penale: portata operativa del divieto e ruolo nell'attuale conflitto tra i poteri dello Stato*, in La *Giustizia penale*, 4/2012, p. 180 ss.; DONINI, *Fattispecie o case law? La "prevedibilità del diritto" e i limiti alla dissoluzione della legge penale nella giurisprudenza*, in *Questione giustizia*, 4/2018, p. 79 ss.; FIANDACA, *Il diritto penale tra legge e giudice*, Cedam, 2002; VASSALLI, voce *Analogia nel diritto penale*, in *Dig. disc. pen.*, vol. I, Torino, 1987.

[308] Sul punto e specificamente sulla critica a quella che viene definita, in opposizione al principio di offensività, una nozione "*metodologica-legittimista*" del bene giuridico tale da "*travestire di esso ogni scelta storica d'incriminazione*" Cfr. DONINI, *Il principio di offensività. Dalla penalistica italiana ai programmi europei*, in *Diritto penale contemporaneo*, 4/2013, p. 7 ss..

A parere di chi scrive viene attuata, in nome di un'interpretazione estensiva, un'operazione analogica, di "*libertinaggio ermeneutico*"[309], mediante la quale si riplasma il concetto di "cosa mobile" sganciandolo dalla specificità della condotta di cui dovrebbe essere l'oggetto.

In questo modo viene costruita una concezione atomistica dell'elemento cosa[310], che è normativizzato: si trasforma l'oggetto materiale in oggetto giuridico del reato, identificandolo con il valore patrimoniale che anche il dato informatico può avere in virtù di "*un vuoto gioco di specchi che si rimandano l'un l'altro ingannevolmente*"[311].

Analoghe distorsioni connotano l'interpretazione sistematica dell'art. 624 c.p. operata alla luce della circostanza del furto o indebito utilizzo dell'identità digitale: si attribuiscono a questa aggravante effetti che la previsione non ha e che anzi il legislatore sembra volutamente non avergli conferito.

Tralasciando la considerazione della patrimonializzazione dell'identità digitale che sarebbe stata operata e che attiene ancora al piano assiologico, come è stato messo in evidenza il legislatore del 2013 nella previsione dell'aggravante ha inteso riferirsi all'art. 30-bis del d.lgs. n. 141 del 2010[312] e quindi all'ipotesi- distinta dal delitto di furto- della c.d. impersonificazione[313]. La previsione, poi, anche dell'indebito utilizzo consente di estendere l'operatività dell'aggravante oltre "*all'apprensione*

---

[309] In questi termini MICHELETTI, J*us contra lex. Un campionario dell'incontenibile avversione del Giudice penale per la legalità*, in *Criminalia*, 2016, p. 170, che indica come tale l'applicazione analogica, spacciata per estensiva, mediante la quale si estrapolerebbe dalla fattispecie originaria una nuova completamente fuori controllo, come sarebbe, ad esempio, accaduto per le molestie olfattive. Su questa tema in generale Cfr. MARINUCCI, *L'analogia e la "punibilità svincolata dalla conformità alla fattispecie penale"*, in *Riv. it. dir. proc. pen*., 2007, p. 1254 ss..

[310] In termini analoghi con riferimento alla riconduzione delle onde elettromagnetiche alla contravvenzione punita dall'art. 674 c.p. GIZZI, *Inquinamento elettromagnetico e responsabilità penale: la Cassazione sul caso Radio vaticana*, *cit*., p. 5 per cui "*La nozione di cosa, allora, deve essere ricostruita in funzione del singolo modello di reato delineato dal legislatore, ricevendo significato dal peculiare contesto linguistico in cui è inserita*".

[311] Testualmente con riferimento all'individuazione del bene giuridico protetto dal delitto di accesso abusivo ad un sistema informatico BERGHELLA, BLAIOTTA, *Diritto penale dell'informatica e beni giuridici*, in *Cass. pen*., n. 9/1995, p. 2331, per cui bisogna invece "*volgersi al bene giuridico non come ad un'eloquente sintesi verbale del paradigma normativo bensì come al compendio dei tratti essenziali ed indefettibili della fenomenologia cui la fattispecie si indirizza*".

[312]MILONE, *La tutela dell'identità digitale nella nuova circostanza aggravante del delitto di frode informatica*, in *Legislazione penale*, n. 1-2/2014, p. 137.

[313] Questa disposizione definisce, ai fini della prevenzione, sul piano amministrativo delle frodi nel settore del credito al consumo, come furto d'identità: "*a) l'impersonificazione totale: occultamento totale della propria identità mediante l'utilizzo indebito di dati relativi all'identità e al reddito di un altro soggetto. L'impersonificazione può riguardare l'utilizzo indebito di dati riferibili sia ad un soggetto in vita sia ad un soggetto deceduto; b) l'impersonificazione parziale: occultamento parziale della propria identità mediante l'impiego, in forma combinata, di dati relativi alla propria persona e l'utilizzo indebito di dati relativi ad un altro soggetto, nell'ambito di quelli di cui alla lettera a)*".

illecita dei dati personali", comprendendovi ogni "*uso «deviato» o «non autorizzato» di dati lecitamente raccolti*"[314], da cui consegua, però, un ingiusto profitto con altrui danno[315].

In considerazione di quanto sopra non è possibile trarre alcuna effetto sistematico che muti, a fattispecie invariata, il modo d'intendere l'oggetto del furto.

2.1.2 In prospettiva de iure condendo

A parere di chi scrive, un furto di dati informatici non appare nemmeno predicabile in prospettiva *de iure condendo* per ragioni fenomenologiche, data la peculiarità delle manifestazioni concrete che identificano il fatto preesistente al "tipo giuridico"[316].

Come messo in evidenza da autorevole dottrina, con riferimento in generale ai dati informatici si pone la questione della rilevanza penale delle ipotesi di "*riproduzione, copia illegittima, cancellazione, trasmissione per via telematica dei dati stessi*"[317], quali condotte che vanno ad incidere sull'altrui diritto di godimento e controllo esclusivo[318], diverso da quello di proprietà o dal possesso e non coincidente

---

[314] Testualmente MALGIERI, *La nuova fattispecie di "indebito utilizzo d'identità digitale": un problema interpretativo*, in *Diritto Penale Contemporaneo Rivista trimestrale*, 2/2015, p. 147, secondo il quale "*solo così le due condotte sono pienamente alternative, poiché il disvalore del fatto consiste nella violazione del consenso del titolare dei dati, che si può realizzare una sola volta: o al momento dell'apprensione dei dati o al momento di un uso deviato di dati lecitamente appresi*".

[315] MALGIERI, *Il furto di identità digitale: una tutela patrimoniale della personalità*, in FLOR, FALCINELLI, MARCOLINI (a cura di), *La giustizia penale nella rete. Le nuove sfide della società dell'informatica nell'epoca di internet*, *I Convegno Nazionale del Laboratorio Permanente di Diritto Penale, Perugia, 19 settembre 2014*, DipLab editore, 2015, p. 41. In questi termini anche CRESCIOLI, *La tutela penale dell'identità digitale*, in *Diritto Penale contemporaneo Rivista trimestrale*, n. 5/2018, p 272, la quale specifica che "*la tutela dal co. 3 art. 640- ter c.p. non può quindi operare per quei casi di furto o indebito utilizzo dell'identità digitale altrui che non sfocino in una diminuzione patrimoniale, ma che ad esempio comportino un'offesa all'onore o alla reputazione della vittima*".

[316] Per tale si intende la fattispecie come fatto descritto dalla disposizione incriminatrice, quello che viene definito come "tipo criminoso" da PAPA, *Fantastic Voyage. Attraverso la specialità del diritto penale*, Giappichelli, 2019 p. 86; ID., *La tipicità iconografica della fattispecie e l'interpretazione del Giudice. La Tradizione illuministica e le sfide del presente*, in CONTE, LANDINI (a cura di), *Principi, regole, interpretazione. Contratti e obbligazioni, famiglie e successioni. Scritti in onore di Giovanni Furgiuele*, p. 337 per cui "*Come rivela dunque la radice semantica del suo essere speciale, la fattispecie si caratterizza - in questa visione a base etimologica - come uno strumento concettuale capace di rispecchiare e trasmettere, tramite la descrizione del fatto tipico, 'la visione', la figurazione di un quadro di vita*". In generale sulla corrispondenza nel diritto, e specificatamente nel diritto penale, del concetto di fatto giuridico o fattispecie a quello di *Tatbestand*, elaborato in seno alla dottrina tedesca, vedi CATAUDELLA, *voce Fattispecie*, in *Enc. dir.*, XVI, 1967, p. 926; Contra GALLO, *Il dolo. Oggetto e accertamento*, *cit.*, p. 278 e nota 19 , per cui il fatto tipico non potrebbe ridursi alla conformità alla fattispecie legale, abbracciando sia gli elementi positivi ma anche quelli negativi; VASSALLI, *Il contributo di Filippo Grispigni alla teoria dell'elemento oggettivo del reato*, in *La Scuola positiva*, 1956, p. 367 ss., il quale ripercorrendo le tesi del GRISPIGNI evidenzia come l'insigne Maestro, riprendendo la concezione del DELITALIA e di esponenti della dottrina tedesca, come BELING, concepisca il fatto tipico come la materialità del reato quale descritta dalla fattispecie legale. Sull'evoluzione della concezione del fatto di reato nella dottrina italiana su influsso di quella tedesca vedi FIORELLA, *Lo sviluppo in Italia, nel '900, delle fondamentali categorie del diritto penale alla luce delle influenze della dottrina tedesca*, in *Rivista it. per le scienze giuridiche*, 6/2015, p. 173 ss..

[317] PICOTTI, *Reati Informatici,* in *Enc. giur. Treccani, Aggiornamento, VIII,* Roma, 2000, p. 2

[318] PICOTTI, *Studi di diritto penale dell'informatica, cit.,* p. 113.

neppure con le condizioni che impongono la tutela del segreto o della riservatezza personale[319]. Questo diritto in senso lato assume le sembianze di un potere di signoria inteso "*quale possibilità di accesso e di godimento indisturbato dei dati, anche qualora siano memorizzati su un supporto altrui. Viene così a rilevare non il luogo o lo spazio (fisico o virtuale) su cui i dati sono stati salvati, bensì l'accessibilità agli stessi e la possibilità di controllarli in modo esclusivo, vale a dire di accedervi liberamente e in forma autonoma e di utilizzarli a proprio piacimento*"[320].

Che la componente dell'accesso al dato sia essenziale ai fini dell'apprensione è confermato da quella stessa dottrina che nel sostenere l'introduzione di un delitto di furto di dati informatici lo ha ricostruito in termini di duplicazione del dato altrui avente valore economico, commessa violando le misure di sicurezza poste a sua protezione[321].

Questa tesi ritiene possibile ascrivere la duplicazione al furto in forza del passaggio della disponibilità del dato che è comunque conseguita dall'agente, ancorché senza contestuale privazione della vittima[322]. In questo modo il disvalore del reato viene identificato nel trapasso da una sfera di disponibilità all'altra, generando, però, un delitto di furto monco del momento usurpativo e distinguibile dalle fattispecie a tutela del segreto e della riservatezza per la riferibilità a questi delitti della mera visione[323].

Tralasciando i rischi di incertezze e sovrapposizioni che conseguono ad una differenziazione così labile, una ricostruzione di questo tipo tradisce la sostanza propria del delitto di furto, concependo come tale quelle forme di intrusione/ingerenza che sono già incriminate nel nostro ordinamento ai sensi dell'art. 615 ter c.p.[324].

Questa disposizione, come autorevolmente precisato, non costruisce il delitto di accesso abusivo ad un sistema informatico o telematico sul momento conoscitivo ovvero acquisitivo del dato "*né tanto meno si tratta di salvaguardare (soltanto) la riservatezza (del contenuto interpersonale dei) dati in essi contenuti, ben potendo, come si è detto, venire in rilievo informazioni già note o prive di per sé di alcuna rilevanza per il titolare. Il valore o interesse da proteggere consiste piuttosto nell'assicurare a ciascuno l'utilizzo o godimento indisturbato ed esclusivo di questi spazi anche solo virtuali*"[325].

---

[319] PICOTTI, *Reati Informatici, cit.*, p. 21.

[320]Testualmente con riferimento alla condotta di detenzione di materiale pedopornografico SALVADORI, *I reati di possesso. Un'indagine dogmatica e politico-criminale in prospettiva storica e comparata*, *cit.*, p. 91

[321] In questi termini SCOPINARO, *Internet e reati contro il patrimonio*, *cit.*, p. 162.

[322] SCOPINARO, *op. cit.*, p. 132.

[323]SCOPINARO, *op. cit.*, p. 159.

[324] Per BERGHELLA, BLAIOTTA, *Diritto penale dell'informatica e beni giuridici*, *cit.*, p. 2332, "*l'art. 615-ter elimina per così dire in radice i pericoli paventati dai sostenitori della necessità di penalizzare il c.d. furto di informazioni, giacché il pirata per impadronirsi delle informazioni contenute in un computer deve necessariamente penetrare o mantenersi illecitamente nel sistema così violando la norma che vieta l'accesso*".

[325] Così SALVADORI, *I reati contro la riservatezza informatica*, in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime*, *cit.*, p. 662. Vedi sulla funzione che le misure di sicurezza hanno secondo la dottrina nella struttura del fatto tipico e sull'utilità di una specificazione normativa della loro portata in ragione del ruolo svolto

Premesso che il riferimento ad un sistema informatico o telematico include vari e differenti spazi di memoria/archiviazione, che vanno dall' "*architettura client-server(….)* [a] *strutture peer-to-peer basate su interazioni tra diversi client senza l'intermediazione di un server centrale*"[326], guardando all'ipotesi della perdita della chiave privata, conseguente alla violazione dei dispostivi o dello spazio virtuale protetto, in cui è allocata dal suo titolare, ne deriva che dalla protezione di un differente "*interesse super-individuale o di natura collettiva al lecito, regolare e corretto utilizzo dei sistemi informatici nonché accesso a spazi informatici, dati e informazioni*"[327] non nasce un problema di vuoto di tutela, ma di anticipata e indiretta tutela che le valute virtuali conseguono.

La fattispecie dell'accesso abusivo costituisce, infatti, un tipico delitto ostacolo, in quanto è volta a punire condotte prodromiche alla commissione di più gravi reati ovvero consistenti nella successiva rivelazione o utilizzazione del dato carpito in un ambito digitale riservato[328].

Rispetto a questo quadro, differente questione da porsi è se in prospettiva *de iure condendo* sia auspicabile la previsione, con riferimento a questo delitto, di una circostanza aggravante costruita sulla funzione del dato quale strumento per un'operatività "patrimoniale", come può essere appunto la chiave privata che sia stata acquisita in virtù dell'accesso, ovvero, alla luce delle perdite patrimoniali che ne possano conseguire, di un'aggravante di evento di danno patito dalla vittima.

Questa verifica non dovrebbe essere operata tanto o solo a fini dell'incremento in sé del trattamento sanzionatorio, prevedendo le fattispecie nazionali già per le ipotesi base pene in generali più elevate di quelle previste dalle disposizioni sovranazionali[329], quanto per giovare alla descrizione del fatto

dall'utente CASALE, *Prima "legge" della sicurezza informatica: "un computer sicuro è un computer spento"*, in *Archivio penale*, 2/2021, p. 5 ss..

[326] CASTAGNO, STIGLIANO, *L'accesso abusivo a sistema informatico nell'era delle tecnologie dell'informazione e della comunicazione*, in *Diritto di internet*, n. 4/2019, p. 791, che chiariscono espressamente che "*il riferimento è in particolare al fenomeno del blockchain quale database distribuito basato proprio sulla decentralizzazione delle funzioni di norma affidate al server centrale*".

[327] FLOR, *Verso una rivalutazione dell'art. 615 ter c.p.?*, in *Diritto Penale contemporaneo Rivista trimestrale*, n. 2/2012, p. 135. Per l'Autore "*da un lato è innegabile che una componente di tale "area riservata" riguardi la facoltà, il potere, il diritto del titolare di gestire in modo autonomo le utilità e le risorse del sistema informatico, nonché i contenuti delle comunicazioni informatiche (o telematiche), indipendentemente dalla loro natura; dall'altro lato appare indispensabile un bilanciamento con le esigenze connesse alla sicurezza informatica*".

[328] SEMINARA, *Note sul reato di accesso abusivo a sistemi informatici o telematici da parte di un pubblico agente (art. 615-ter, c. 2, n. 1, c.p.)*, in *Rivista di diritto dei media*, n. 2/2018, p. 10.

[329] L'art. 9 della direttiva 713/2019 indica per i reati di cui alle lett. a) e b) degli artt. 4 e 5 la pena detentiva massima non inferiore a due anni, che sale a 5 anni per tutti i reati contemplati dalla direttiva in esame che siano commessi nell'ambito di un'organizzazione criminale quale definita nella decisione quadro 2008/841/GAI. Le corrispondenti fattispecie nazionali fissano in misura superiore a 3 anni la misura massima della reclusione base, che è innalzata a 5 anni nelle ipotesi aggravate.

tipico, al fine di meglio rappresentarne l'attitudine offensiva[330], che può anche indirizzarsi verso interessi di tipo economico-patrimoniale[331].

Proprio alla luce della prospettiva indicata, nessuna delle due proposte sembra percorribile: la prima opzione finirebbe per generare rigidismi incompatibili con la rapidità dello sviluppo tecnologico, nonché dubbi sulla funzione della conoscibilità del dato, che è nella costruzione della fattispecie base irrilevante[332]; la seconda comporterebbe rischi di sovrapposizione ed ineffettività, essendo plausibile che l'evento di danno sia previsto quale requisito della fattispecie di utilizzazione da cui deriva in via diretta, come accade nel caso della frode informatica[333].

In conseguenza di quanto sopra, si ritiene preferibile evitare coloriture patrimoniali anche solo circostanziali che, nel tentativo di esternalizzare un'attitudine offensiva eventuale, finirebbero per alterare l'identità strutturale ed assiologica della fattispecie, compromettendone la già labile coerenza rispetto alla sua collocazione codicistica[334].

In conclusione, deriva per il penalista la necessità di apprestare una tutela del dato informatico di rilevanza patrimoniale al di fuori delle maglie del furto, evitando commistioni anche sole

---

330 Con riferimento all'art. 615 ter c.p. contestano sia l'entità della cornice edittale, sia in generale l'efficacia dissuasiva della norma, CASTAGNO, STIGLIANO, *op. ult. cit.*, i quali ritengono che nella realtà, in base alla tipologia dello spazio virtuale oggetto di accesso abusivo, l'autore del fatto potrebbe conseguire il potere "*di influenzare amplissime aree della vita di un individuo con conseguenze potenzialmente gravissime, risultando in una forma di attacco alla libertà personale piuttosto che all'inviolabilità del domicilio. Se è vero che la vittima di tale accesso abusivo potrà invocare la tutela dell'art. 615 ter c.p., la lievità della cornice edittale ("fino a tre anni"), segno di una limitata percezione dell'offensività del reato, non appare adeguata a fronte della amplissima attitudine lesiva di tali condotte*".

331 In proposito Cass. pen., Sez. V, 1.10.2008, n. 37322, con nota di FARINA, in *Diritto penale e processo*, n. 6/2009, p. 719 ss., relativamente alla duplicazione da parte di due professionisti dei *files* dello studio in cui avevano lavorato, ha precisato, che l'art. 615 ter c.p. tutela "*secondo la più accreditata dottrina, molti beni giuridici ed interessi eterogenei, quali il diritto alla riservatezza, diritti di carattere patrimoniale, come il diritto all'uso indisturbato dell'elaboratore per perseguire fini di carattere economico e produttivo, interessi pubblici rilevanti, come quelli di carattere militare, sanitario nonché quelli inerenti all'ordine pubblico ed alla sicurezza, che potrebbero essere compromessi da intrusioni o manomissioni non autorizzate. Tra i beni e gli interessi tutelati non vi è alcun dubbio, come già osservato dalla Suprema Corte (Cass., Sez. 6 penale, 4 ottobre 1999 - 14 dicembre 1999, n. 3067, CED 3067), che particolare rilievo assume la tutela del diritto alla riservatezza e, quindi, la protezione del domicilio informatico, visto quale estensione del domicilio materiale. Tanto si desume dalla lettera della norma che non si limita soltanto a tutelare i contenuti personalissimi dei dati raccolti nei sistemi informatici, ma prevede uno ius excludendi alios quale che sia il contenuto dei dati, purché attinenti alla sfera di pensiero o alla attività lavorativa dell'utente; è, quindi, evidente che da tale norma vengono tutelati anche gli aspetti economici e patrimoniali, come si è dinanzi anticipato*";

332 FLOR, *Il diritto penale alla prova dell'hands-on dell'ethical hacking*, nota a Tribunale di Catania, Gip Rizza, decreto di archiviazione 15 luglio 2019, in *Diritto di internet*, n. 1/2020, p. 167, per cui "*dalla lettera della norma, infatti, appare evidente che il legislatore abbia inteso sanzionare l'accesso abusivo e la mera permanenza non autorizzata nel sistema e non, invece, le attività poste in essere contestualmente, non assumendo rilevanza, ai fini della consumazione dell'illecito de quo, l'effettiva presa di conoscenza di dati o informazioni e nemmeno le motivazioni che hanno mosso il soggetto agente*". *Contra* F. MANTOVANI, *Diritto penale, parte speciale*, cit., p. 575, secondo cui l'accesso abusivo consiste nella conoscenza dei dati contenuti nel sistema informatico.

333 Vedi in proposito paragrafo 3.3.

334 Per ONORATI, COZZA, *I reati in tema di comunicazioni*, in PARODI, SELLAROLI (a cura di), *Diritto penale dell'informatica. Reati della rete e sulla rete*, cit., p. 367, la tutela apprestata dall'art. 615 ter c.p. non riguarda il "domicilio informatico", ma il libero e genuino accesso ai dati e sistemi informatici.

circostanziali ed indirizzando l'intervento verso quelle fattispecie inerenti agli spazi e ai sistemi di sua conservazione e transito.

2.2 Al cospetto del delitto di appropriazione indebita.

Sulla base del primo comma dell'art. 646 c.p., il delitto di appropriazione indebita sussiste in caso di appropriazione, per procurare a sé o ad altri un ingiusto profitto, del denaro o della cosa mobile altrui di cui già si abbia, a qualsiasi titolo, il possesso[335].

La sussistenza di questa previa disponibilità comporta che, diversamente dal furto, l'appropriazione costituisca, ad avviso di scrive, un'ipotesi di usurpazione mediante "consolidamento"[336] o, come autorevolmente sostenuto in dottrina, di espropriazione-impropriazione[337], quale c.d. interversione di un preesistente possesso[338] da cui consegua l'esclusione volontaria e definitiva del titolare del bene con acquisizione a favore proprio o di terzi[339].

Confermativa in questo senso sarebbe la strutturazione del reato sia sul momento acquisitivo, che ne determina la consumazione al compimento di atti di signoria[340], sia l'espressa qualificazione d'ingiustizia che connota il profitto[341]. Con riferimento a questo profilo "*la distanza dalla «semplice» realità della sottrazione, che tangibilmente manifesta la globale ingiustizia del fatto di furto, determina, quindi,*

---

[335] Sulla ricostruzione del dibattito dottrinale sulla definizione della nozione di possesso quale *actio finium regundorum* rispetto al delitto di furto si rinvia a A. LANZI, *voce furto*, in *Enc. giur. Treccani*, XIV, Roma, 1989, p. 5 ss.; ANTOLISEI, *Manuale di diritto penale, parte speciale*, *cit*., p. 398, lo definisce, invece, come "*relazione tra la persona e la cosa, che consente alla prima di disporre della cosa in modo autonomo, e che la disponibilità (o signoria) è autonoma quando si svolge all'infuori della diretta vigilanza di una persona che abbia sulla cosa un potere giuridico maggiore*".

[336] Con consolidamento si intende l'assenza in questo reato di un momento propriamente espropriativo in senso materiale di sottrazione che connota invece il furto; in dottrina in questo senso Cfr. PEDRAZZI, voce *Appropriazione indebita*, in *Enc. dir*., II, Milano, 1958, p. 835, per cui "*Il limite logico del concetto di possesso è precisamente quello di sottrazione: non v'è possesso ogni volta che il soggetto, pur trovandosi in relazione materiale con la cosa, per farla propria deve sottrarla*".

[337] Cfr. PAGLIARO, voce *Appropriazione indebita,* in *Dig. pen*., I, 1987, p 227.

[338] PAGLIARO, *op. ult. cit*.; in termini analoghi AIMI, *In tema di uso e appropriazione nell'ambito dei delitti di peculato,* in *Riv. it. dir. proc. pen.*, 2013, p. 2072.

[339] Nel senso dell'alterazione della destinazione del bene, strumentalizzato a vantaggio dell'agente o di un terzo, BARTOLI, *La distinzione tra appropriazione e distrazione e le attuali esigenze di tutela patrimoniale*, in *Diritto penale e processo*, n. 9/2001, p. 1142.

[340] Sul dibattito dottrinale e giurisprudenziale sul connesso profilo, ai fini della consumazione del reato, dell'ininfluenza della percezione della persona offesa del comportamento incompatibile con il suo diritto posto in essere dall'agente vedi PAOLONI, *Il momento consumativo del delitto di appropriazione indebita,* nota a Cass. pen. sez. II, 10.04.2014, n.17901, in *Cassazione penale*, n. 4/2015, pp. 1449 ss.

[341] *Contra* SICCARDI, *Il "fine di profitto" nei delitti contro il patrimonio*, *cit*., p. 363, che invece concepisce l'attributo dell'ingiustizia quale connotazione immanente nella nozione di profitto anche nei reati, come il furto, in cui manca tale indicazione esplicita.

il bisogno di compensare il mancato richiamo alla «cosa», quale termine di convergenza «materiale» del conflitto di interessi, con un'espressa qualificazione in termini di antigiuridicità"[342].

In questo modo, ad avviso di chi scrive, si supplisce, in generale, anche alla genericità della condotta di appropriazione, che può risultare, oltre che non facilmente percepibile *ab externo* in conseguenza della previa disponibilità dell'oggetto in capo all'autore[343], di non facile definizione in presenza di ipotesi come quelle di uso o di distrazione della cosa.

In proposito la dottrina è divisa tra chi considera dette ipotesi incompatibili con l'appropriazione, intesa quale impossessamento definitivo[344], e chi, invece, le ammette[345].

A sostegno dell'ammissione è stata valorizzata l'incidenza invasiva che l'uso o la distrazione hanno sulla *res*, che le renderebbe sostanzialmente coincidenti con "*un atto di signoria assoluta*"[346], od ancora la loro contrarietà rispetto al titolo del possesso ovvero all'interesse del proprietario[347], per cui "*soltanto il possessore che rompe il rapporto tra il bene e il proprietario e lo impiega contro l'interesse del medesimo, disconosce la signoria e quindi si comporta uti dominus*" [348]:

Questa tesi è sostanzialmente condivisa dalla giurisprudenza, la quale- ai fini della distinzione tra furto e appropriazione indebita- considera decisiva l'indagine circa il potere di disponibilità sul bene

---

[342] PICOTTI, *Il dolo specifico. Un'indagine sugli "elementi finalistici" delle fattispecie penali*, *cit*., p. 246.

[343] PONTEPRINO, *La "dubbia" configurabilità dell'appropriazione indebita d'uso*, in *Diritto penale e processo*, n. 1/2021, p. 91, considera il verbo appropriarsi un dato normativo estremamente generico ed ontologicamente ambiguo, che prescinde da qualsiasi riscontro in *rerum natura*.

[344]PONTEPRINO, *op. cit.*, p. 96, per cui "*ogniqualvolta il legislatore abbia voluto sanzionare l'uso non consentito della cosa altrui ha previsto un'apposita fattispecie delittuosa. Peraltro, la scelta di tipizzare il furto e il peculato d'uso e non, invece, l'appropriazione indebita d'uso non può certo essere tacciata di irragionevolezza; in effetti, tanto l'art. 626, n. 1, quanto l'art. 314, comma 2, c.p. reprimono fenomeni criminosi espressivi di un disvalore più elevato: nel primo caso il momentaneo godimento del bene altrui è preceduto da un'azione sottrattiva mentre, nel secondo, la peculiare qualifica soggettiva ricoperta dell'agente e la natura pubblicistica del bene giuridico protetto giustificano la maggior tutela apprestata dall'ordinamento giuridico*".

[345] BARTOLI, *La distinzione tra appropriazione e distrazione e le attuali esigenze di tutela patrimoniale*, *cit*., p. 1143, secondo cui "*l'espropriazione della appropriazione si ha quando non solo risulta alterato il vincolo strumentale, ma sussiste anche la definitiva rottura della relazione tra il proprietario e la cosa, situazione che si può verificare anche con l'uso della stessa*".

[346] TESTA, *Appropriazione indebita*, in FIORE (a cura di), *I reati contro il patrimonio*, *cit*., p. 341, definisce come tali "*quelle condotte di uso che comportano necessariamente un atto di signoria assoluta sul bene, tale da porsi in contrasto con i diritti del proprietario per la particolare natura del comportamento, o per la rilevante diminuzione patrimoniale nella sfera del vero dominus*".

[347]TESTA, *Appropriazione indebita*, *cit*., p. 342, per cui "*dunque, ai fini del reato de quo, è certamente possibile affermare che la condotta posta in essere debba mostrarsi almeno incompatibile con la destinazione impressa dal dominus sulla res, secondo il titolo per cui lo stesso la possiede, ed essere, inoltre, causa di una dismissione definitiva del bene, lesiva degli interessi del proprietario della cosa che avvenga in forme corrispondenti all'esercizio delle facoltà del proprietario, pregiudicando la relazione funzionale tra quest'ultimo ed il bene di riferimento*". In termini corrispondenti GUIDI, *Appropriazione, distrazione ed uso nel delitto di peculato*, Milano, 2008, p. 137.

[348] Così BARTOLI, *La distinzione tra appropriazione e distrazione e le attuali esigenze di tutela patrimoniale*, cit., p. 1146, che definisce conformemente la condotta appropriativa di cui agli artt. 646 e 314 comma 1 c.p. "*sottrazione definitiva (irrevocabile, irreversibile) del bene o uso arbitrario del bene accompagnato dalla certezza obiettiva che il bene non potrà essere recuperato (momento espropriativo), e impiego del bene a proprio vantaggio o di un terzo e contro l'interesse del proprietario (momento impropriativo).*

da parte dell'agente[349] e ritiene sussistente l'appropriazione nel caso del mancato rispetto dei limiti in ordine alla sua utilizzabilità[350], mentre irrilevante è considerato, ai fini della sussistenza del reato, il legame fiduciario o di affidamento[351].

Riferendo questa condotta così delineata all'oggetto, la Suprema Corte lo ha concepito in termini fisici-corporali, escludendo, analogamente al furto, i beni immateriali e i dati informatici, salvo ancora una volta la loro incorporazione in supporto materiale costituente cosa mobile ai sensi dell'art. 646 c.p.[352].

Si è discostata recentemente da questo orientamento la sentenza 11959/2020 della seconda sezione della Suprema Corte che ha, invece, ritenuto che "i *dati informatici (files) sono qualificabili cose mobili ai sensi della legge penale e, pertanto, costituisce condotta di appropriazione indebita la sottrazione da un personal computer aziendale, affidato per motivi di lavoro, dei dati informatici ivi collocati, provvedendo successivamente alla cancellazione dei medesimi dati e alla restituzione del computer 'formattato'*"[353].

Nello specifico, spinta dalla dichiarata necessità di "adeguare" le categorie giuridiche alle attuali tecnologie informatiche[354], la Corte ha utilizzato essenzialmente due argomenti per giungere alla

---

[349]Per la disamina della giurisprudenza, in particolare di legittimità, si rinvia ad AUGELLO-PESA, *La proprietà del trustee e il reato di appropriazione indebita*, in *Trusts e attività fiduciarie,* n. 4/2015, p. 335 ss.; FERRARI, *La nozione di possesso non cambia pelle nel passaggio dal campo civile al penale*, Nota a Cass. pen., Sez. Un., 27.10.2004, n.1327, in *Diritto e Giustizia*, n. 5/2005, p. 38 ss.; ancorché con riferimento ai confini tra truffa e appropriazione indebita, anche, MAZZANTINI, *Truffa contrattuale- La mancata restituzione del veicolo noleggiato fra truffa e appropriazione indebita*, nota a Cass. pen., Sez. VI, 12.01.2016, n. 1408, in *Giur. It*., n. 7/2016, p. 1749 ss..

[350] Con specifico riferimento all'appropriazione quale impiego dell'oggetto o del denaro in violazione della specifica destinazione di scopo impressa dalla vittima e vincolante per l'autore del reato vedi Cass. pen., Sez. II, 24.10.2017, n. 50672; Cass. pen., Sez. IV, 31.01.2019, n. 8128; Cass. pen., Sez. II, 26.11.2020, n. 37820; Cass. pen., Sez. II, 23 aprile 2021, n. 15566, tutte consultabili alla banca dati on line *www.pluris-cedam.utetgiuridica.it.*

[351]*Contra* F. MANTOVANI, *Diritto penale, parte speciale*, *cit.,* p. 123, il quale discostandosi dall'opinione dottrinale prevalente lo ritiene elemento essenziale che consente di diversificare e giustificare il trattamento sanzionatorio più lieve relativo alle appropriazioni minori.

[352] In proposito Cass. pen., Sez. II, n. 33839, 12.07.2011, n. 251179 e Cass. pen., Sez. V, 30.09.2014 n. 47105, entrambe consultabili alla banca dati on line *www.pluris-cedam.utetgiuridica.it*. Le pronunce indicate sono espressione dell'orientamento per cui, stante l'inidoneità del bene immateriale ad essere suscettibile di fisica detenzione, potrà essere oggetto di appropriazione solo l'entità materiale su cui venga trasfuso, in quanto "*incorporando il bene immateriale, tali entità materiali acquisiscono il valore di questo, diventando cose idonee a soddisfare quei particolari bisogni umani cui il bene è strumentale*". In senso conforme anche Cass. pen., Sez. V, 25.01.2021, n. 3000, che ha censurato la sentenza gravata che aveva ritenuto assorbito l'appropriazione nel delitto punito dall'art. 623 c.p. relativamente alla condotta di un ex dipendente, accusato di aver superato i limiti di utilizzo del personal computer aziendale, servendosi dell'accesso per copiare, abusivamente, a fini personali, i dati riservati della società e poi cancellarli: per la Corte alcuna valutazione è stata compiuta dalla pronuncia impugnata rispetto al complesso dei beni oggetto di appropriazione "*onde verificare se questi abbiano una rilevanza economica propria e/o comunque, ove trasfusi in materiale tangibile, siano possibile oggetto di appropriazione ex art. 646 c.p.*".

[353] Così Cass. pen., Sez. II, 10.04.2020 n. 11959 in *Diritto penale e processo,* 6/2020, con nota di CORBETTA, *I Files sono "cosa mobile"?*, p. 749 ss..

[354] Per Cass. pen., Sez. II, 10.04.2020 n. 11959, *cit*., testualmente "*la ratio, sottesa alla selezione delle classi di beni suscettibili di formare oggetto delle condotte di reato di aggressione all'altrui patrimonio, è agevolmente individuabile nella prospettiva della correlazione delle condotte penalmente rilevanti (essenzialmente, quelle che mirano alla sottrazione della disponibilità di beni ai soggetti che siano titolari dei diritti di proprietà o di possesso sulle cose considerate)*

configurazione nel caso esaminato del delitto di appropriazione: il primo è relativo al riconoscimento della fisicità del dato informatico sulla base delle conoscenze scientifiche; il secondo attiene alla configurabilità nei confronti di questo dato della detenzione, ritenuta necessaria per ravvisare le condotte di sottrazione e impossessamento o appropriazione di cose mobili.

Circa il primo argomento, si ritine che il file "*pur non potendo essere materialmente percepito dal punto di vista sensoriale, possiede una dimensione fisica costituita dalla grandezza dei dati che lo compongono, come dimostrano l'esistenza di unità di misurazione della capacità di un file di contenere dati e la differente grandezza dei supporti fisici in cui i files possono essere conservati e elaborati*"[355].

Per quanto riguarda, invece, il secondo si richiama "*la capacità del file di essere trasferito da un supporto informatico ad un altro, mantenendo le proprie caratteristiche strutturali, così come la possibilità che lo stesso dato viaggi attraverso la rete Internet per essere inviato da un sistema o dispositivo ad un altro sistema, a distanze rilevanti, oppure per essere "custodito" in ambienti "virtuali" (corrispondenti a luoghi fisici in cui gli elaboratori conservano e trattano i dati informatici); caratteristiche che confermano il presupposto logico della possibilità del dato informatico di formare oggetto di condotte di sottrazione e appropriazione*"[356].

Sulla base dell'iter argomentativo seguito dalla Corte, perché si possa considerare sussistente l'appropriazione indebita in ordine ai files è necessaria, inoltre, "*la loro cancellazione, previamente duplicati e acquisiti autonomamente nella disponibilità del soggetto agente*"[357]: solo così viene a sussistere

---

all'attività diretta a spogliare il titolare del bene dalla possibilità di esercitare i diritti connessi all'utilizzazione del bene, è chiaro che la sottrazione (violenta o mediante attività fraudolente o, comunque, dirette ad abusare della cooperazione della vittima) debba presupporre in via logica la disponibilità, da parte dei soggetti titolari, dei beni su cui cade la condotta penalmente rilevante; ma anche in questo contesto deve prendersi atto che il mutato panorama delle attività che l'uomo è in grado di svolgere mediante le apparecchiature informatiche determina la necessità di considerare in modo più appropriato i criteri classificatori utilizzati per la definizione di nozioni che non possono rimanere immutabili nel tempo". In senso favorevole sulla fattibilità e legittimità di questa operazione interpretativa evolutiva CAPPITELLI, *I confini della nozione di bene mobile nei delitti contro il patrimonio*, in *Cassazione penale*, 3/21, p. 931-932, il quale fa leva, essenzialmente, sull'elasticità del concetto di cosa mobile.

[355] In dottrina in senso conforme SCOPINARO, *Internet e reati contro il patrimonio*, *cit.*, p. 112. Con specifico riferimento alla sentenza in esame in senso critico ZANNOTTI, *Appropriazione indebita di "files"? Il "file", come l'aria, è un bene immateriale che può essere concretizzato solo attraverso un supporto*, in *La Giustizia Penale*, 8-9/2020, fasc. 8-9, p. 464 ss..

[356] Ad ulteriore conferma della bontà di questo argomento viene richiamata la "*circostanza per cui anche il denaro (che pur è fisicamente suscettibile di diretta apprensione materiale), nella sua componente espressiva del valore di scambio tra beni, è suscettibile di operazioni contabili, così come di trasferimenti giuridicamente efficaci, anche in assenza di una materiale apprensione delle unità fisiche che rappresentano l'ammontare del denaro oggetto*". Non è possibile condividere questo argomento perché come messo in evidenza da GROSSI, *I tormenti della "cosa mobile" penalmente rilevante: la Corte di cassazione ne estende la portata ai documenti informatici (files)*, in *Giurisprudenza penale web*, 10/2020, p. 7, "*è la natura del denaro che fa sì che una sua sottrazione o impossessamento o trasferimento o appropriazione porti con sé necessariamente un danno al legittimo detentore. Pur volendo incardinare il discorso lungo questo solco, e fermo restando che appare quantomeno difficoltoso riconoscere al file le stesse "caratteristiche" del denaro, è utile notare come il «trasferimento» del file, affinché sia rilevante quale sottrazione e comporti dunque un «danno» al legittimo detentore, esiga l'eliminazione dalla fonte nel quale il file era precedentemente «situato»*".

[357] PISANI, *La nozione di "cosa mobile" agli effetti penali e i files informatici: il significato letterale come argine all'applicazione analogica delle norme penali,* in *Dir. pen. proc.*, 5/2020 , p. 654, che evidenzia in proposito come non sia rispettata la sequenza tipica del delitto di appropriazione indebita perché "*l'espropriazione non precede temporalmente l'impropriazione poiché il file passa nella sfera di signoria dell'agente con l'estrazione indebita dal sistema*

quella definitiva sottrazione del bene patrimoniale al titolare del diritto di godimento ed utilizzo del bene, che è ritenuta necessaria ai fini della sussistenza del reato[358].

In realtà la cancellazione è fatto ulteriore, offensivamente diverso, che nulla ha a che vedere con l'effetto traslativo[359]; la stessa dottrina che è richiamata dalla Corte a sostegno delle sue conclusioni discorre in ipotesi di tal fatta di danneggiamento informatico[360].

A prescindere dai dubbi che solleva un'interpretazione evolutiva che è, in realtà, analogia "mascherata"[361], l'iter argomentativo seguito è censurabile sotto diversi profili. Sembra, ad avviso di chi scrive, che siano forzate le categorie del reato nel tentativo di renderle compatibili con la fisiologica pluricondivisibilità che connota le entità digitali e che impedisce che la mera duplicazione del dato integri quella condotta espropriativa-impropriativa che identifica il delitto di appropriazione[362].

Parte della dottrina è di contrario avviso, ritenendo che già la stessa copiatura del file integri la condotta di appropriazione, in quanto il "*quid proprii del delitto de quo deve ravvisarsi nell'abuso del titolo di possesso, laddove siffatto titolo consiste nella regolamentazione (legale o convenzionale) dei doveri e poteri inerenti la disponibilità fisica e/o giuridica della cosa in cui il possesso consiste (…) se la duplicazione dei file non rientra nel titolo del possesso, perché non contemplata ovvero espressamente vietata nelle pattuizioni genetiche del rapporto possessorio, si verte in abuso del possesso di rilievo penale; se la copia è un utilizzo che lascia intatto il rapporto materiale tra proprietario-cosa (pur riducendo l'esclusività e quindi attenuando il valore economico della res) e tuttavia contrasta con il titolo, integra una delle epifanie dell'appropriazione indebita*"[363].

---

informatico; ma in tale momento l'originario detentore non è privato ancora dell'accesso e uso dei dati informatici in esso racchiusi".

[358] FARINELLA, *La Cassazione sulla configurabilità del reato di appropriazione indebita di files,* in *Indice penale*, 3/2020, p. 718, per cui in questo modo la Corte chiarisce come ai fini della sussistenza del delitto non basta la mera interversione del possesso.

[359] *Contra* CIPOLLA, *L'appropriazione indebita informatica nel contesto della dematerializzazione del concetto di cosa nei reati contro il patrimonio*, in *La Giustizia Penale*, 11/2020, p. 624, secondo cui la copiatura non autorizzata in sé, laddove sorretta da fine di ingiusto profitto, integra il delitto di appropriazione.

[360] SCOPINARO, *Internet e reati contro il patrimonio*, *cit*., p. 131-132.

[361] Diffusamente in proposito BARILE, *Appropriazione indebita di file informatici: tra interpretazione estensiva e divieto di analogia. Il diritto penale è "cosa mobile"*, in *Sistema penale*, 3/21, p. 149, per cui "*l'inclusione dei file informatici tra le 'cose' in considerazione della loro fisica ma non tangibile esistenza appare piuttosto il frutto di una torsione interpretativa ardita che, se assecondata, potrebbe portare agli esiti più disparati, soprattutto in considerazione dell'ampiezza dei possibili significati che il vocabolo 'cose' è suscettibile di abbracciare*".

[362] PISANI, *La nozione di "cosa mobile" agli effetti penali e i files informatici: il significato letterale come argine all'applicazione analogica delle norme penali*, *cit*., p. 653, per cui "*Una corretta enucleazione del bene giuridico protetto, da individuarsi nella relazione fattuale tra soggetto e cosa, rende incompatibile la condotta di sottrazione con la connotazione immateriale del dato informatico. Medesima riflessione può essere svolta riguardo all'impossessamento: l'acquisto della piena ed autonoma disponibilità della cosa mobile sottratta postula l'apprensione fisica e il collocamento della stessa al di fuori della sfera di vigilanza materiale del titolare*".

[363] Testualmente CIPOLLA, *L'appropriazione indebita informatica nel contesto della dematerializzazione del concetto di cosa nei reati contro il patrimonio*, cit., p. 622-623.

La ricostruzione sopra prospettata non sembra però rientrare nella struttura della fattispecie dell'art. 646 c.p.: l'appropriazione è sostanzialmente differente dal mero "abuso" o ancora dal mero inadempimento civilistico, perché questi non generano quella perdita definitiva della disponibilità che identifica la prima. Non è un problema di violazione in sé dei limiti della distribuzione di poteri e facoltà, occorrendo un'"*oggettiva usurpazione, vale a dire unilaterale modificazione del rapporto, a favore del medesimo agente, nel latente conflitto di interesse per il godimento esclusivo del bene*" [364].

La duplicazione, non consentendo di conseguire questa esclusività di godimento, non pregiudica il "possesso" del bene digitale in termini usurpativi, come richiesto dall'art. 646 c.p.. Il richiamo al depauperamento del valore economico della res per co-disponibilità- rispetto a quella del possessore e del titolare- che deriverebbe dalla duplicazione, non basta per la configurabilità del delitto di appropriazione ed afferisce, peraltro, ad una dimensione assiologica, includente profili di riservatezza e segretezza, differenti da quelli patrimoniali[365].

3. L'utilizzazione senza diritto e a vantaggio proprio o altrui e il possibile corrispondente nazionale.

Da quanto sopra risulta che il nucleo identificativo del delitto di appropriazione indebita è l'impropriazione in funzione usurpativa del titolare, generativa di una relazione esclusiva in capo all'autore rispetto ad una *res* fisicamente intesa. Nonostante la valorizzazione dell'atto di "impiego" ai fini dell'usurpazione, la natura reale della fattispecie non sembra poter essere messa indubbio. Questa dimensione è predominante rispetto all'abuso, che, nell'ottica del legislatore del '30, ha una valenza strumentale e non identificativa, in conformità ad una ricchezza circolante di tipo materiale. Sulla base, invece, delle indicazioni sovranazionali[366], l'"*utilizzazione senza diritto a vantaggio proprio o di altri*" è il contenuto identificativo, da un punto di vista modale e sostanziale, di un delitto avente un contenuto di "appropriazione", che con riferimento alle valute virtuali dovrebbe, peraltro, avere ad oggetto le chiavi private nella loro funzione di "*mezzo per disporre del "bene" e che, grazie alle sue particolarità, permette allo stesso di entrare nella sua disponibilità*"[367].

Non bisogna, infatti, dimenticare che i *virtual asset* sono "*rappresentazioni digitali di valore*", con la conseguenza che chi acquisisce il controllo delle chiavi private assume il potere di eseguire e giovarsi di trascrizioni criptate sulla blockchain mediante le quali attuare scambi digitali o realizzare altrimenti il corrispettivo del loro valore.

---

[364] PICOTTI, *Il dolo specifico. Un'indagine sugli "elementi finalistici" delle fattispecie penali*, *cit.*, p. 245.
[365] PICOTTI, *La tutela penale della persona e le nuove tecnologie dell'informazione*, in PICOTTI (a cura di), *Tutela penale della persona e nuove tecnologie*, Padova, 2013, p. 29 ss..
[366] Si rinvia in proposito al capitolo III.
[367] CAPACCIOLI, *Riflessioni sulla tassazione delle criptovalute: wallet quale deposito?*, *cit.*, p. 67

La strutturazione della formulazione sovranazionale dell'ipotesi di appropriazione indebita è conforme a questa oggettività, oltre che particolarmente idonea a reprimere possibili abusi che possono essere commessi dai *wallet provider* che non si limitino ad erogare solo servizi di custodia, ma anche di vera e propria gestione delle chiavi private[368]. La varietà dei servizi oggi offerti dai providers è, infatti, tale che appare limitativo distinguere semplicemente tra *exchange* e *wallet provider*, potendo i differenti e combinati servizi essere resi dalla medesima piattaforma[369]. Ferma, pertanto, la necessità di procedere caso per caso alla disamina del contenuto d'ingerenza sull'operatività del cliente, ad eccezione dei casi in cui è solo fornito il dispositivo-programma per operare, senza alcun controllo sulla chiave privata, negli altri casi il *provider* ha una disponibilità che laddove abusata può effettivamente generare per il titolare la perdita o comunque l'indisponibilità di quanto investito o conservato in valute virtuali.

In generale, non potendo preventivare il futuro sviluppo di questo mercato, ulteriori potrebbero essere i casi in cui venga ceduta la chiave privata e chi sia chiamato ad operare per conto terzi abusi delle possibilità conferite, "espropriandolo" del "potere" di operare e di giovarsi degli scambi digitali, attuabili in virtù delle trascrizioni criptate.

Per le ragioni sopra esposte, nonostante la denominazione formale di "appropriazione indebita" sembra possibile in prospettiva *de iure condendo* valorizzare le indicazioni sovranazionali che vanno oltre la previsione dell'art. 646 c.p., la quale viene considerata da autorevole dottrina "*non in grado di tutelare il patrimonio rispetto a modalità di aggressione emergenti da una realtà economico sociale sempre più artificiale*"[370].

Disposizione idonea in questo senso sembra, invece, l'art. 493 ter c.p. ed, in particolare, il delitto d'indebito utilizzo di uno strumento di pagamento diverso dal contante.

Come autorevolmente rappresentato[371], questa fattispecie consente la repressione anche di quelle infedeltà che siano state commesse dal terzo violando i limiti di uso a lui consentiti.

---

[368] Si rinvia sul punto alla nota 107.

[369] In questo senso CAPONERA, GOLA, *Aspetti economici e regolamentari delle «cripto-attività»*, in *Questioni di Economia e Finanza (Occasional Papers)* di Banca d'Italia, n. 484, Marzo 2019, p. 36, per cui "*è opportuno parlare in modo più generale di soggetti che offrono servizi per "valute virtuali" senza una precisa distinzione*", potendo trattarsi di in maniera combinata di *order-book exchange, virtual currency exchange, brokerage service, multilateral trading platform, centralized exchange/custodian wallet provider, payment processing* e finanche gestione di ATM e altri servizi, come carte di debito opzionali per effettuare acquisti diretti in valuta virtuale.

[370] BARTOLI, *La distinzione tra appropriazione e distrazione e le attuali esigenze di tutela patrimoniale*, *cit.*, p. 1148

[371] In questi termini GALANTE, *La tutela penale delle carte di pagamento*, in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime, cit.*, p. 296, che discorre in generale dell'incriminazione mediante la prima parte del primo comma dell'art. 493 ter c.p. delle ipotesi appunto di infedeltà da parte dell'utilizzatore legittimato.

Al pari dell'abusività che connota l'art. 615 ter[372] c.p., la locuzione avverbiale "indebitamente" costituisce, infatti, elemento identificativo del fatto tipico[373] esprimente la contrarietà ai vincoli dispositivi[374] imposti al soggetto non titolare dello strumento di pagamento[375]. Diversamente da quanto sostenuto da un parte della dottrina[376], questa locuzione non può essere concepita come una clausola "*d'illiceità-antigiuridicità espressa*"[377], che nulla aggiungerebbero al disvalore del fatto di reato, limitandosi a richiamare l'attenzione del giudice sull'assenza di cause di giustificazione.

Letta, unitamente al requisito del dolo specifico del fine di profitto[378], l'avverbio "indebitamente" riferito, in particolare, al terzo che abbia ricevuto la carta dal suo titolare[379], assume un'identità

---

[372] Sul ruolo che questo elemento ha ai fini della descrizione del fatto tipico e della definizione della sua illiceità si rinvia a SALVADORI, *Quando un insider accede abusivamente ad un sistema informatico o telematico? Le Sezioni Unite precisano l'ambito di applicazione dell'art. 615 ter c.p.*, in *Riv. trim. dir. pen. econ.*, 1-2/2012, p. 369 ss.; ID., *I reati di possesso. Un'indagine dogmatica e politico-criminale in prospettiva storica e comparata*, *cit.*, p. 117-118; in termini sostanzialmente analoghi anche MASSI, *Speciale anti-doverosità della condotta ed elusione del fatto tipico*, Giappichelli, 2020, p. 73 ss., che discorre di requisiti di anti-doverosità espressa che arricchiscono "*il significato di disvalore*".

[373] Nel senso del conferimento a clausole di tal fatta del ruolo di fattore di tipizzazione Cfr. MORGANTE, *Note critiche in tema di illiceità espressa e speciale*, in DE FRANCESCO (a cura di), *Scritti in onore di Antonio Cristiani*, 2002, p. 569 ss.; ID., *L'illiceità speciale nella teoria del reato*, Torino, 2002, p. 141 ss..

[374] PICOTTI, *Reati Informatici, cit.*, p. 9, chiarisce come mediante la locuzione avverbiale viene operato il rimando a tutte le norme extrapenali anche di fonte pattizia/regolamentare che disciplinano l'impiego della carta.

[375] GALANTE, *op. ult. cit.*.

[376] In questo senso proprio con riferimento alla fattispecie in esame e alla portata scriminante ai sensi dell'art. 50 c.p. del consenso del titolare della carta si rinvia a D'AGOSTINO, *La tutela penale dei mezzi di pagamento della terza generazione*, *cit.*, p. 414, per cui in questo modo "*le conseguenze civili connesse al comportamento di chi permette al terzo di utilizzare la propria Carta Bancomat resterebbero invariate, mentre, invece, sul piano penalistico la repressione risulterebbe limitata alle sole condotte non coperte dal consenso dell'avente diritto*".

[377] In tal senso PULITANÒ, *Illiceità espressa e illiceità speciale,* in *Riv. it. Dir. proc. pen.*, 1967, p. 65 ss., il quale distingue queste clausole da quelle d'"illiceità speciale" in cui l'illiceità derivi da una norma extrapenale diversa da quella incriminatrice. Sui legami che sussisterebbero tra questi elemento del fatto e l'antigiuridicità vedi RISICATO, *Gli elementi normativi della fattispecie penale, Profili generali e problemi applicativi,* Giuffrè, 2004, p. 102 ss., la quale li considera, pur nella necessità di una verifica caso per caso, assimilabili- come tecnica di normazione e funzione agli elementi normativi.

[378] GALANTE, *La tutela penale delle carte di pagamento*, *cit.*, p. 297-298, secondo cui si tratta di "*un elemento che consente di risolvere almeno due tipologie di casi problematici. Nell'ipotesi di utilizzo della carta da parte del già titolare, quindi dopo la revoca della stessa o dopo la scadenza del contratto, il fine di profitto richiesto dalla disposizione consente di restringere l'ambito di applicazione della fattispecie «ai casi di soggetto non titolare, poiché soltanto chi opera al di fuori di qualsiasi rapporto negoziale agisce nella convinzione di non assumere obbligazioni di sorta a lui imputabili e di ricavarne un profitto». La seconda tipologia di casi consiste nell'utilizzazione di una carta bancomat altrui per effettuare un prelievo nell'interesse del proprietario, ma senza che il soggetto sia stato previamente autorizzato dal titolare stesso. Anche in questa ipotesi manca il fine di profitto per sé o per altri, dovendosi intendere «per altri tutti i soggetti diversi dal titolare della carta»*".

[379] Di recente sul punto Cass. pen. Sez. II, 25-09-2020, n. 26807, con nota di VADALÀ, *La dimensione finanziaria delle valute virtuali. Profili assiologici di tutela penale*, in *Giur. it.*, 10/21, p. 2224 ss., per cui "*la legittimazione all'impiego del documento è contrattualmente conferita dall'istituto emittente al solo intestatario, il cui consenso all'eventuale utilizzazione da parte di un terzo è del tutto irrilevante*"; in senso analogo anche Cass. pen., Sez. II, 12.05.2021 n. 18609, in www.giurisprudenzapenale.it del 19 maggio 2021, in base alla quale "*l'autorizzazione assumerà rilevanza solo nelle ipotesi in cui sia apprezzabile in modo manifesto (attraverso la dimostrazione dei rapporti esistenti tra le parti e delle circostanze in cui sia intervenuta l'autorizzazione) che il terzo utilizzatore dello strumento di pagamento o di prelievo di denaro agisce solo nell'interesse del titolare, eseguendo materialmente le operazioni consentite con l'uso della carta di credito, su disposizione del titolare legittimo*".

specifica ai fini della definizione del disvalore del reato, evidenziando la strumentalizzazione dell'autorizzazione del titolare all'utilizzo della carta, quale condotta tipica ai sensi dell'art. 493 ter c.p., proprio perché mezzo diretto a conseguire in tal modo un guadagno indebito, in conflitto con l'interesse protetto.

Salvo i casi in cui il terzo operi come 'longa manus' o mero esecutore di un'operazione non comportante la sottoscrizione di alcun atto e che non può sfuggire in alcun modo al dominio del soggetto legittimato[380], l'utilizzo dello strumento di pagamento da parte di soggetto non titolare è per la giurisprudenza penalmente rilevante, in quanto costituente la "*lesione del diritto incorporato nel documento, del quale il solo titolare può disporre in modo esclusivo*"[381].

Con riferimento agli strumenti di pagamento che siano forniti in forza di accordi contrattuali o da intermediari "tradizionali", la previsione del fine di profitto, richiedendo la strumentalità del mezzo oggettivo al perseguimento del fine soggettivo[382], evita che l'illiceità del fatto venga a coincidere con l'inadempimento civilistico.

3.1 Il delitto d'indebito utilizzo di strumenti di pagamento diversi dai contanti in rapporto all'utilizzazione fraudolenta.

[380] Cfr. Cass. pen. Sez. II, 22/02/2019, n. 17453, consultabile alla banca dati *Pluris on line*, in forza della quale "*Anche l'uso di una carta di credito da parte di un terzo, autorizzato dal titolare, integra il reato di cui all'art. 12, d.l. 3 maggio 1991, n. 143, convertito nella legge 5 luglio 1991, n. 197 (ora art. 493-ter cod. pen.), in quanto la legittimazione all'impiego del documento è contrattualmente conferita dall'istituto emittente al solo intestatario, il cui consenso all'eventuale utilizzazione da parte di un terzo è del tutto irrilevante, stanti la necessità di firma all'atto dell'uso, di una dichiarazione di riconoscimento del debito e la conseguente illiceità di un'autorizzazione a sottoscriverla con la falsa firma del titolare, ad eccezione dei casi in cui il soggetto legittimato si serva del terzo.*

[381] In questi termini Cass. Sez. I, 5-11-2002 n. 37115 con nota di SCOPINARO, *Acquisto e utilizzo illeciti di carta di credito via internet*, *cit.*, per cui "*L'ipotesi in esame, dunque, prescinde dal possesso del documento e si realizza con l'addebito in banca a carico del titolare del documento e il contestuale raggiungimento del profitto dell'utilizzatore con la conclusione del negozio giuridico con la controparte cui l'importo dell'«operazione» è accreditato via Internet.; canale quest'ultimo che costituisce un mezzo e un modo di realizzazione del delitto di cui trattasi, si è, all'evidenza, al di fuori di un'applicazione analogica, non consentita, della norma penale*".

[382] Cfr. PICOTTI, *Il dolo specifico. Un'indagine sugli "elementi finalistici" delle fattispecie penali*, *cit.*, p. 501. Con specifico riferimento al dolo specifico del delitto in esame si veda anche ROSSI, *Per l'integrazione del reato di cui all' art. 493-ter c.p. non occorre il conseguimento di un profitto o il verificarsi di un danno*, in *Cassazione penale*, 10/2019, p. 3653 ss.. Si segnala nella giurisprudenza recente sul modo d'intendere il predetto requisito Cass. pen., sez. II 17.02.2021, n. 6184/2021, consultabile all'*Osservatorio Cybercrime https://sites.les.univr.it/cybercrime/* alla sezione *Frodi e abusi di carte di credito*, per cui "*non ricorre affatto ipotesi di reato impossibile, per inidoneità dell'azione, in quanto il D.Lgs. n. 231 del 2007, art. 55, comma 9, (ora art. 493 ter c.p.) punisce la condotta di chi "al fine di trarne profitto per sè o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento"; il profitto è dunque oggetto di dolo specifico, che non necessariamente deve realizzarsi ai fini della integrazione del reato, mentre la condotta punibile è l'indebito utilizzo di una carta di credito o di pagamento (quale certamente è la carta carburanti (OMISSIS)) da parte di chi non ne è titolare; sicché l'indebito utilizzo prescinde dalla conoscenza o dalla disponibilità del codice di accesso o dalla sua immissione in un apparecchio bancomat destinata al altri scopi, oltre che dal concreto conseguimento del profitto, - che deve animare l'agire, ma non necessariamente deve realizzarsi ai fini della integrazione della fattispecie*".

Dall'analisi condotta risulta confermata che la fattispecie d'indebito utilizzo di carta di credito o di pagamento è sostanzialmente corrispondente ad una condotta "abusiva" di utilizzazione in funzione usurpativa.

Lo schema del decreto legislativo che dovrebbe dare attuazione alla direttiva UE/2019/713, ad eccezione dell'ampliamento dell'oggetto materiale del reato, non prevede alcuna innovazione della struttura di questo delitto; appare, pertanto, necessario verificare se esso sia idoneo ad incriminare anche quella condotta di utilizzazione fraudolenta, che il legislatore sovranazionale costruisce come differente e successiva rispetto a quella "acquisitiva" esaminata.

In proposito si segnala che la giurisprudenza[383] e parte della dottrina[384] occupandosi dei rapporti tra il delitto di truffa e l'indebito utilizzo hanno finito per attribuire a quest'ultimo una connotazione fraudolenta ritenendo che "*l'adozione di artifizi o raggiri è [*sia*] uno dei possibili modi in cui si estrinseca l'uso indebito di una carta di credito*"[385]. In considerazione di quanto sopra alcune pronunce hanno negato il concorso di reati, ritenendo il delitto di truffa assorbito nel più grave reato d'indebito utilizzo[386]; altre, invece, lo hanno ammesso "*ogni qualvolta la condotta incriminata non si esaurisca nel mero utilizzo di essi, ma sia connotata da un "quid pluris" concretantesi in artifici e raggiri*"[387].

Ad avviso di chi scrive va preferito quest'ultimo orientamento: pur essendo possibile attribuire all'indebito utilizzo una funzione anche di governo della "circolazione" degli strumenti di pagamento per contrastare le frodi, il delitto nazionale rimane focalizzato sul momento dell'abusività dell'operato del terzo, funzionale al perseguimento del fine profitto.

Proprio questo fine, quale "*polo teleologico di un unitario comportamento esterno, di cui puntualizza la globale tipicità*"[388], indirizza la fattispecie verso una dimensione differente dallo "sfruttamento" consapevole e volontario della falsità od origine illecita del mezzo di pagamento, a cui sembra

---

[383] L'indirizzo a cui si fa riferimento è stato inaugurato alla già citata Cass. pen., Sez. un., 28 marzo 2001, n. 22902, per cui si rimanda per un esame specifico degli aspetti qui considerati ZACCAGNINI, *Note sull'art. 12 della l. n. 197/91, quale "disposizione di chiusura" della normativa di compliance italiana e suoi rapporti con il delitto di ricettazione*, in *Cass. pen.*, 1/2002, p. 318 ss..

[384] Cfr. C. PECORELLA, *Il nuovo diritto penale delle «carte di pagamento», Il nuovo diritto penale delle "carte di pagamento"*, in *Riv. it. dir. proc. pen.*, 1993, p. 286.

[385] In questi termini Cass. pen., Sez. II, 21.06.2017, n. 33526, consultabile alla banca dati on line *www.pluris-cedam.utetgiuridica.it*., la quale discorre di rapporto tra le due norme di "*specie a genere*".

[386] Tra queste vedi Cass. pen. Sez. II, Sent., 04.12.2015, n. 48044; Cass. pen. Sez. II, 20.06.2013, n. 26865, consultabile alla banca dati on *line www.pluris-cedam.utetgiuridica.it.*

[387]In questo senso Cass. pen., Sez. fer., 12.12.2011, citata da CHIARI, *Uso indebito di carte di credito e truffa: concorso di reati o assorbimento*?, in *Quotidiano Giuridico* del 4 agosto 2017, che ritiene che "*le sentenze che escludono l'assorbimento, in favore del concorso di reati, non si pongano in contrasto con il dictum della massima composizione del Supremo Collegio, ma ne valorizzino appieno il contenuto, nella parte in cui si individua la soluzione dell'alternativa concorso apparente di norme/concorso di reati nel valutare se l'adozione di artifici o raggiri […] si identifichi nell'uso indebito, sì da potersi parlare di un'unica condotta prevista contemporaneamente da due norme incriminatrici, ovvero costituisca condotta tutt'affatto diversa, sì da far luogo all'applicazione di entrambe*".

[388] Testualmente PICOTTI, *op. cit.*, p. 502.

riferirsi proprio l'obbligo d'incriminazione dell'utilizzazione fraudolenta[389]. Il dolo specifico di profitto consente, cioè, di farne emergere la peculiare offensività che connota l'operato dell'agente nel conflitto con l'interesse del titolate della carta, in una prospettiva di tutela principalmente patrimoniale-individuale. In questo senso confermativa è la stessa origine del delitto d'indebito utilizzo, che era quella d'incriminare gli "abusi" delle carte bancomat, che venivano illegittimamente ricondotti in via analogica al furto aggravato dall'uso del mezzo fraudolento[390], nonostante la sottrazione della carta non fosse equiparabile a quella di "«*una chiave*» *utilizzata per sottrarre denaro custodito in una cassaforte, non avendo una funzione meramente protettiva, bensì una attiva, idonea ad eseguire l'adempimento della banca*" [391].

Ne deriva che una conforme attuazione nazionale dell'obbligo d'incriminazione dell'utilizzazione fraudolenta avrebbe richiesto l'introduzione di un corrispondente delitto o, eventualmente la previsione alternativa, rispetto all'"indebitamente", del requisito della "fraudolenza".

Questa requisito, solo laddove inteso, secondo quanto qui proposto[392], come effetto sui terzi di un'utilizzazione che sia diretta a provocare effetti dannosi senza far emergere la connotazione illecita dello strumento o metodo utilizzato, avrebbe, infatti, potuto contribuire ad intercettare normativamente quelle ipotesi effettivamente lesive della sicurezza degli scambi perché dirette a giovarsi dell'ignoranza del terzo su quanto viene effettivamente ricevuto in pagamento o a titolo di scambio o di realizzazione del valore digitale.

Per essere più chiari, i termini del conflitto che andrebbero riferiti all'utilizzazione fraudolenta interessano direttamente la posizione dell'agente in rapporto a coloro che vengono in contatto con lo strumento di pagamento oggetto dello scambio. Quanto sopra appare indiscutibile con riferimento a strumenti di pagamento falsificati o alterati, ma lo è di fatto anche per quelli di origine altrimenti illecita, in quanto è innegabile che l'evoluzione delle tipologie di strumenti di pagamento esistenti e soprattutto la loro diffusività e la facilità d'impiego abbiano fatto emergere interessi ulteriori, direttamente bisognosi della garanzia di un corretto e sicuro utilizzo.

La fraudolenza come qui concepita, riflettendosi anche sull'elemento psicologico, che deve consistere nella consapevole volontà di "sfruttare" la peculiare connotazione dell'oggetto dell'utilizzazione, è, quindi, ultronea rispetto al fine di profitto, che è, invece, l'elemento normativo di tutti i reati previsti dall'art. 493 ter c.p.

[389] Si rinvia in proposito al paragrafo 3.2.
[390] PICOTTI, *Reati Informatici, cit.*, p. 8.
[391] Testualmente PICOTTI, *Studi di diritto penale dell'informatica, cit.*, p. 91.
[392] Si rinvia in proposito al cap. III.

3.2. Le altre fattispecie dell'art. 493 ter c.p. e la tecnica di normazione prescelta

L'art. 493 ter c.p. è concepita come una "*figura criminosa multiforme*"[393], prevedendo nella seconda parte del primo comma anche i reati di falsificazione, alterazione, nonché possesso, cessione e acquisizione di strumenti di pagamento contraffatti, alterati o di provenienza illecita.

Questi reati sono stati strutturati analogamente al delitto d'indebito utilizzo. In questo modo, però, alimentandosi i dubbi sulla loro consistenza assiologica, essi sono ricondotti ora in via esclusiva alla fede pubblica[394], conformemente alla collocazione codicistica[395] nel capo III delle "*falsità in atti*"[396], del titolo VII, del libro II del codice penale, ora al patrimonio[397], ora cumulativamente ad entrambe, in virtù dell'affermata plurioffensività[398].

Lo schema del decreto legislativo di attuazione della direttiva UE/2019/713 non prevede alcun correttivo sul punto, risultando, così, anche queste fattispecie non perfettamente conformi alla funzione di tutela che è alla base degli obblighi sovranazionali d'incriminazione delle condotte c.d. "connesse"[399].

---

[393] In questo Corte Cost. con la sentenza 302/2000, le cui statuizioni sono state di fatto riprese da Cass. pen., Sez. un., 28.03.2001, n. 22902, in *Cass. pen.*, 2002, con nota di FAIELLA, *Offesa e sanzione del cd. riciclaggio di carte di credito,* p. 119 ss..

[394] In dottrina per il riferimento quale bene giuridico tutelato da questo delitto alla fede pubblica SCOPINARO, *Internet e reati contro il patrimonio*, cit., p. 74-75.

[395] Con questa collocazione operata dal d.lgs. n. 21/2018, è stata smentita la connessione di questa disposizione con il sistema antiriciclaggio, al cui interno era stata in origine collocata. In questo senso esplicita è proprio la Relazione governativa allo schema del decreto legislativo n. 21/18. Conformemente in dottrina vedi LAZZONI, *la fattispecie di indebito utilizzo, falsificazione, alterazione di carte di credito e di pagamento*, in BERNASCONI, GIUNTA (a cura di), *Riciclaggio e obblighi dei professionisti*, Giuffrè, 2011, Milano, p. 189-190.

[396] Sulla composizione ed in generale sul contenuto di questo capo vengono avanzate riserve e critiche a partire dalla sua coerenza interna, raccogliendo fattispecie eterogenee e non essendo chiaro a monte quali siano le diverse categorie di atti tutelati. In questo senso vedi DE MARISCO, *voce Falsità in atti*, in *Enc. Dir.*, XVI, Milano, 1967, p. 565; CISTERNA-LARUSSA, *I delitti di falso*, Cedam, 2010, p. 141 ss..

[397] Per la natura di delitto contro il patrimonio vedi BERTOLINO, *Nuovi orizzonti dei delitti contro il patrimonio nella circonvenzione di incapace e nell'usura*, cit., p. 24 e nota 46, che richiama anche la circostanza che disposizione analoga a quella nazionale è collocata nell'ambito dei delitti contro il patrimonio sia nel codice penale svizzero che in quello spagnolo.

[398] Si esprime in questo senso GALANTE, *La tutela penale delle carte di pagamento*, in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime, cit.*, p. 285 Considerazioni assiologiche analoghe vengono operate con riferimento alle fattispecie nazionali di falso nummario, che sono generalmente reputate in dottrina a tutela della certezza e dell'affidabilità del traffico monetario, nonché, in considerazione delle implicazioni macroeconomiche conseguenti ad un eccesso di moneta circolante e dei danni patrimoniali a carico dei privati ingannati dal falso monetario, di altri interessi meritevoli di tutela. Vedi in questo senso SPINA, *Nuove norme in materia di tutela penale dell'euro*, in www.legislazionepenale.eu del 27 dicembre 2016; mentre disconosce in toto il ruolo della fede pubblica quale bene giuridico, proponendo il trasferimento delle fattispecie di falso nummario nell'ambito dei reati contro l'economia, COCCO, *Il falso bene giuridico della fede pubblica*, in *Riv. it. dir. proc. pen.*, 1/2010, p. 80.

[399] Si rinvia in proposito al paragrafo 3 del cap. III.

Nello specifico, l'ampliamento del loro oggetto non è sufficiente in assenza di altre modifiche a renderle effettivamente compatibili sia con questa rinnovata oggettività, sia con l'obiettivo sovranazionale di tutela perseguito.

Con riferimento al primo aspetto, lo schema del decreto non sostituisce il riferimento al possesso con la detenzione, che sarebbe stata più appropriata per gli strumenti di pagamento immateriali, e non contempla nemmeno nessuna condotta di quelle che il legislatore europeo riferisce in maniera eterogena all'obbligo d'incriminare l'atto di procurare per sé e per altri[400].

In proposito, si segnala che, pur avendo le fattispecie nazionali di cessione e acquisto una carica modale ampia, sarebbe stato "fenomenologicamente" opportuno il riferimento almeno alla vendita, data la sussistenza di un vero e proprio "mercato", raggiungibile con facilità on line, dei codici delle carte di credito o dei dati di autenticazione ed operatività di diversi servizi di pagamento[401].

Sul piano, invece, dei requisiti di queste fattispecie, lo schema del decreto mantiene, ancora una volta analogamente all'indebito utilizzo, il dolo specifico di profitto.

Questa scelta è particolarmente censurabile con riguardo alle condotte di falsificazione e alterazione, rispetto alle quali il fine di profitto non può essere idoneo fattore di selezione[402] di condotte che andrebbero represse in quanto lesive della genuinità dello strumento di pagamento in sé, a prescindere dalla sua consistenza monetaria o materiale. Questo requisito, che non è previsto a livello sovranazionale, opera una non dovuta restrizione dell'area del penalmente rilevante, generando dubbi sull'identità di queste fattispecie.

In realtà, la stessa conclusione vale anche per gli altri reati di possesso, cessione e acquisizione, rispetti ai quali risulta essere opportuna la strutturazione a dolo specifico, ma non il contenuto del fine.

Anche per queste condotte la ragione sostanziale della loro incriminazione alla luce della direttiva UE/2019/713 andava riferita alla loro strumentalità diretta a consentire la circolazione da vietare, perché avente ad oggetto strumenti di pagamento contraffatti o comunque di provenienza illecita. Confermativo in questo senso è il riferimento espresso da parte della direttiva, ancorché solo per la condotta di detenzione dello strumento di pagamento immateriale, al requisito intellettivo della rappresentazione della sua origine illecita al momento della ricezione[403].

---

[400] Si rinvia in proposito alle note 171 e 178.

[401] Sulla diffusività di "mercati" di questo tipo, di recente, vedi https://www.repubblica.it/cronaca/2021/01/20/news/dark_web_ecco_quanto_costano_carte_di_credito_identita_paypal-283480625/.

[402] Vedi in generale su questa funzione che viene attribuita al dolo specifico MAZZACUVA, *Il disvalore di evento nell'illecito penale: l'illecito commissivo doloso e colposo*, Giuffrè, Milano, 1983, p. 231.

[403] Si rinvia sul punto alle note 236.

Lo schema del decreto legislativo in esame non solo non ha previsto l'introduzione di questo requisito, né tantomeno la condotta di detenzione, ma ha anche lasciato invariato il fine di profitto, indirizzando così i reati di possesso, cessione e acquisizione verso un orizzonte di tutela diverso o comunque certamente più ridotto di quello che sarebbe stato riferibile all'adozione del fine previsto dalla norma sovranazionale di utilizzazione fraudolenta.

Analogamente al dolo specifico di messa in circolazione di monete contraffatte o alterate[404], questo fine avrebbe dovuto essere preferito, nel suo ruolo di fattore di selezione dei comportamenti meritevoli di sanzione penale, anche per la maggiore specificità e determinatezza che lo connota rispetto a quello assai ampio di profitto.

La tendenza della giurisprudenza ad identificare quest'ultimo anche come mera "*utilità di tipo morale*"[405], già con riferimento agli stessi delitti contro il patrimonio, rende ancora più distonico questo fine rispetto alla collocazione e corrispondente funzione di tutela che dovrebbe attribuirsi alle fattispecie in esame.

La sua mancata previsione per i reati della seconda parte dell'art. 493 ter c.p., oltre a giovare alla loro coerenza complessiva, avrebbe permesso di differenziarli sostanzialmente dal delitto di ricettazione.

Rispetto a quest'ultimo delitto, sulla base delle previsioni dello schema del decreto legislativo di attuazione della direttiva UE/2019/713, unico elemento specializzante dovrebbe continuare ad essere solo l'oggetto materiale della condotta, che oltre di provenienza illecita[406], potrebbe avere natura immateriale[407].

Da quanto sopra deriva che rispetto, invece, ad uno strumento di pagamento materiale di provenienza delittuosa, sulla scia dell'orientamento prevalente in giurisprudenza, dovrebbe continuare ad ammettersi la configurabilità anche del delitto di ricettazione nel caso di ricezione e successivo utilizzo di carta di provenienza delittuosa, che sia stata contraffatta da terzi, mentre in quello di realizzazione monosoggettiva unica dovrebbero trovare applicazione solo le fattispecie dell'art. 493 ter c.p., in concorso tra loro[408].

---

[404] Si rimanda alle note 203, 204 e 206 per l'analisi del contenuto che viene attribuito a questa ipotesi di dolo specifico relativamente, in particolare, alle fattispecie nazionali di acquisto e ricezione di monete contraffatte o alterate.

[405] Così SICCARDI, *Il "fine di profitto" nei delitti contro il patrimonio*, *cit.*, p. 359; in termini analoghi sulla propensione della giurisprudenza e di una parte della dottrina ad applicare dette norme incriminatrici anche quando non siano in gioco interessi economici, né patrimoniali in senso più lato VALLINI, *La sottrazione violenta di ovociti e le torsioni del "tipo criminoso"*, in *Giur. It.*, 7/2021, p. 1732.

[406] In questo senso AMATO, *Solo nei casi di "provenienza delittuosa" l'acquisto di carte di credito è ricettazione - La punibilità dell'illecito utilizzo esclude il ricorso con il reato di truffa*, in *Guida al diritto*, 29/2001, p. 58 ss..

[407] Si rinvia per la definizione del contenuto multiplo che è assegnato a livello normativo alla nozione di strumento di pagamento immateriale alle note 164 e 165.

[408] *Di recente in proposito* Cass. pen., Sez. II, 17.02.2021, n. 6195, consultabile all'*Osservatorio Cybercrime https://sites.les.univr.it/cybercrime/* alla sezione *Frodi e abusi di carte di credito*, per cui: "*Risponde dei reati di ricettazione e di indebito utilizzo di carte di credito di cui all'art. 493 ter, comma 1, prima parte, c.p., il soggetto che, non*

Sotto questo profilo, come qui auspicato, lo schema del decreto in esame conferma la costruzione dell'art. 493 ter c.p. quale "disposizione a più norme"[409], integrando le figure criminose, rispettivamente, di indebito utilizzo, falsificazione o alterazione, possesso, cessione o acquisizione di carte di credito di provenienza illecita, "*attesa l'eterogeneità, sotto l'aspetto fenomenico, dei rispettivi caratteri, differenti ipotesi di reato, tra le quali è configurabile il concorso*"[410].

Per essere più chiari questa disposizione è ricondotta alla categoria delle norme penali miste cumulative, in cui ciascuna condotta corrisponde ad un'autonoma fattispecie[411].

Premesso che la distinzione rispetto alla norma penale mista alternativa[412] è una questione essenzialmente interpretativa "*dovendosi stabilire se la legge resti indifferente o meno, sul piano della commisurazione della pena, alla realizzazione congiunta di più ipotesi*"[413], rispetto ad una disposizione come l'art. 493 ter c.p. la giurisprudenza nazionale ha ritenuto, comunque, possibile discorrere di reato unico "*sebbene integrato sotto l'aspetto materiale da una pluralità di condotte*" in presenza del riscontro positivo "*cumulativo di un'identità oggettiva (devono avere uno stesso oggetto materiale), soggettiva (devono essere compiute dallo stesso soggetto), cronologica (devono essere contestuali) e psicologico-funzionale (devono essere indirizzate verso un unico fine) tra le diverse condotte penalmente sanzionate. Al di fuori del perimetro così delineato, ciascuna violazione della disposizione incriminatrice si tradurrà, al contrario, in altrettanti reati quante siano state le condotte effettivamente realizzate dall'agente*"[414].

---

avendo concorso nella realizzazione della falsificazione, riceve da altri carte di credito o di pagamento contraffatte e faccia uso di tale mezzo di pagamento; mentre risponde delle due autonome ipotesi di reato previste dall'art. 493 ter, comma 1, c.p., in concorso, l'autore della contraffazione che proceda anche all'utilizzo indebito di questo mezzo di pagamento". In senso conforme anche Cass. pen., Sez. II, Sent., 26.05.2021, n. 20834, consultabile alla banca dati on line *www.pluris-cedam.utetgiuridica.it.* Per un'analisi critica di questo orientamento sorto con riferimento a questo reato quando era ancora previsto dall'art. 12 del d.l. 143/1991 si rinvia a DE AMICIS, *Contrasti giurisprudenziali in tema di "ricettazione" di carte di credito*, in *Cass. pen.*, 9/2000, p. 241 ss..

[409] Vedi per la sua definizione la nota 218.

[410] In questi termini, riprendendo l'orientamento giurisprudenziale inaugurato dalle Sez. un., 28 marzo 2001, n. 22902, PEDULLÀ, *Osservazioni a Cass. Pen., Sez. Sez. V, data udienza Ud. 12 gennaio 2018, data deposito (dep. 20 aprile 2018), n. 17923*, in *Cass. pen.*, 10/2018, p. 3209.

[411] In questo senso in giurisprudenza vedi Cass. pen., sez. II, 18.11.2019, n. 46652, consultabile alla banca dati on line *www.pluris-cedam.utetgiuridica.it*.

[412] Relativamente all'art. 659 c.p. discorre di *mischstrafgesetze* o norme penali miste PUGLISI, *Gestori di pubblico esercizio e omesso impedimento dei rumori degli avventori*, nota a Cass. pen., sez. III, 2 luglio 2019, n. 28570, in *Giur. it.*, 1/2020, p. 185 e nota 35, il quale definisce la norma mista alternativa o a più fattispecie quale disposizione che contiene un'unica norma incriminatrice applicabile indifferentemente alle varie modalità di condotta previste, sia che ne sia posta in essere una o più di una tra quelle elencate.

[413] Testualmente PASCALE, *Circostanze-Il concorso tra più circostanze tipizzate al n. 1 3° comma dell'art. 628 c.p.*, nota a Cass. pen. Sez. II, 09.10.2020, n. 29792, in *Giur. It.*, 5/2021, p. 1198, per cui i criteri determinanti per stabilire quale sia la natura di una norma penale mista dovrebbero essere quelli di ragionevolezza e proporzionalità della risposta sanzionatoria.

[414] Così Cass. pen. sez. II, 17 gennaio 2014, n. 1856, consultabile alla banca dati on line *www.pluris-cedam.utetgiuridica.it*., con riferimento alle disposizioni dell'art. 642 c.p., che è considerata "*norma penale mista del tutto peculiare, giacché accorpa in sé sia la qualifica di disposizione a più norme (nel rapporto tra le condotte previste nei commi 1 e 2) sia quella di norma a più fattispecie (in riferimento alle condotte previste all'interno di ciascun comma)*".

La *ratio* di questo orientamento, che si condivide, va ricercata nel tentativo di escludere la pluralità di reati ogni qual volta ad essere unica è la carica offensiva della specifica manifestazione criminale, che, ancorché fenomenologicamente plurima, è espressione di una conflittualità univocamente direzionata.

Laddove nel caso di realizzazione monosoggettiva ciò non si verifichi, i singoli reati commessi che siano avvinti dal nesso di "connessione", indicato dalla disposizione sovranazionale[415], saranno, comunque, considerabili in termini unitari ai fini della valutazione della responsabilità dell'agente e della proporzionale quantificazione della pena.

Nello specifico, l'unicità del disegno criminoso[416] richiesto dall'art. 81 c.p., comma 2, per il trattamento di favore previsto per i reati in continuazione, potrà, infatti, riflettere- laddove inteso in chiave progettuale come "*conglomerato di condotte psichicamente vissute dal reo in modo unitario, in relazione alla loro funzionalità rispetto a un obiettivo finale*"[417]- quella strumentalità ad un fine ultimo, che è alla base di detto nesso di "connessione", quale finalismo anche soggettivo all'utilizzazione dello strumento illecitamente acquisito.

Con riguardo all'apprensione illecita degli strumenti di pagamento dematerializzati rimane, invece, complessa, in considerazione degli interventi che sono indicati dallo schema del decreto legislativo di attuazione della direttiva UE/2019/713, la definizione dei rapporti con il delitto di frode informatica[418], il quale riveste certamente un ruolo centrale nella protezione del patrimonio in un sistema di scambi digitali ed è punito meno severamente dell'art. 493 ter c.p..

---

[415] Vedi sul punto il paragrafo 3 del capitolo III.

[416] Per ZAGREBELSKI, *voce Reato continuato*, *cit*., p. 844, essendo l'unicità del disegno criminoso che giustifica la disciplina di favore dell'art. 81 c.p., deve trattarsi della previa rappresentazione dell'offesa tipica dei singoli reati che saranno posti in essere per la realizzazione del programma di azione criminoso. Di recente CANATO, *Il reato associativo mafioso e la continuazione con i reati scopo*, in *Giurisprudenza penale web*, 5/2020, p. 5-6, discorre, conformemente all'indirizzo maggioritario teleologico-programmatico, di prefigurazione mentale accompagnata dall'elemento finalistico dell'unicità dello scopo dell'intero programma delinquenziale.

[417] Testualmente GABOARDI, *Le loquaci spoglie del reato continuato*, in *Cass. pen*., 11/2014, p. 3996, che giustifica il trattamento sanzionatorio previsto dall'art. 81 c.p. in considerazione della progettazione psichica unitaria che avvince i vari reati e che ne giustifica la valutazione congiunta in sede di accertamento della colpevolezza.

[418] La giurisprudenza, pur concordando sull'individuazione-quale elemento differenziale che determinerebbe la ricorrenza della sola frode informatica- dell'utilizzazione fraudolenta del sistema informatico, appare divisa sui casi in cui essa sarebbe ricorrente: alcune pronunce ritengono sufficienti la mera digitazione dei codici in servizi on line, altri richiedono un *quid pluris*. Per un esame dei termini di questo contrasto si rinvia a LEO, *Sulla qualificazione dell'utilizzo abusivo nel circuito informatico dei codici concernenti carte di credito*, in *Diritto Penale e Processo*, 6/2013, p. 660 ss.. Come recente espressione del secondo orientamento indicato vedi Cass., sez. II, 1° luglio 2020, n. 21831 in *Diritto di internet*, 4/2020, con nota di GUERRA, D'ANELLO, p. 177 ss.. Con questa pronuncia la Corte ha ribadito, il principio espresso in altri precedenti che "*in ipotesi di utilizzo di carte con banda magnetica falsificata, acquisizione illegittima dei codici segreti di accesso al sistema bancario, inserimento senza diritto nel sistema stesso, ordine di pagamento, con intervento sui dati contabili del sistema, ipotesi nelle quali rientra la fattispecie concreta oggetto del ricorso in esame, è ravvisabile solo il reato di frode informatica, in quanto l'elemento specializzante costituito dall'utilizzazione fraudolenta del sistema informatico costituisce presupposto assorbente rispetto alla generica indebita utilizzazione di una carta di credito, iscritta, come ratio, nel novero di misure destinate al controllo dei flussi finanziari, in funzione di prevenzione del riciclaggio*". In senso critico sull'atteggiamento ambivalente

Ad esso merita, dunque, di essere dedicato il successivo paragrafo.

3.3 Il delitto di frode informatica: possibili modifiche superflue in prospettiva di tutela della sicurezza informatica

Introdotto con la legge 23 dicembre 1993, n. 547 nel titolo XIII, capo II "*dei delitti contro il patrimonio mediante frode*", per valorizzare la vicinanza rispetto alle fattispecie comuni preesistenti[419], questo delitto è volto ad incriminare quelle ipotesi in cui l'azione fraudolenta, volta a carpire un atto di disposizione patrimoniale, incide direttamente sul funzionamento di un sistema informatico o telematico o viene attuata mediante intervento senza diritto sui dati, informazioni e programmi in esso contenuti[420].

Di conseguenza una parte della dottrina ha ritenuto che, nonostante l'ambigua denominazione[421], la fattispecie prevista dall'art. 640 *ter* c.p. costituisca un'ipotesi di aggressione unilaterale aggravata dal peculiare mezzo[422].

Questo orientamento non è condivisibile perché finisce per eclissare la nota identificativa del fatto tipico: l'alterazione o l'intervento senza diritto- in qualsiasi modo ovvero con qualsiasi modalità

---

della Corte ed in generale per l'esclusione del concorso con operatività del solo delitto d'indebito utilizzo vedi FALDUTI, *Frode informatica e utilizzo indebito di carte di credito: variabili interpretative*, in *Giurisprudenza penale web*, 12/2017, p. 1 ss., ed in particolare p. 10 per cui "*dal punto di visto sistematico, inoltre, apparirebbe poco funzionale sottoporre ad una fattispecie con pena più grave e una procedibilità d'ufficio, le ipotesi di possesso, falsificazione, detenzione e cessione di carte di credito (tutte condotte realizzabili da remoto e senza materialità della carta), e al contempo, nel caso di utilizzo, ricomprendere tutto il paradigma fattuale appena richiamato nel novero di un generico "intervento senza diritto su dati", applicando l'art. 640 ter c.p. con una pena più bassa, e solo laddove sia soddisfatta la condizione di procedibilità. Per le ragioni sopraesposte, la condotta di chi, ottenuti i dati relativi ad una carta di credito, indebitamente li utilizzi, non essendone titolare, come metodo di pagamento al fine di trarne profitto, appare meglio adattarsi all'ipotesi di reato di cui all'art. 55 d. lgs. 231/2007*".

[419] In questo senso criticamente PICOTTI, *Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale, cit.*, p. 190, per cui né è derivato un quadro normativo non soddisfacente.

[420] Sulla definizione dell'oggetto e delle modalità di questo delitto si rinvia a MARGIOCCO, *Frode informatica*, in FINOCCHIARO, DELFINI (a cura di), *Diritto dell'informatica*, Assago, 2014, p. 1107 ss.; MINICUCCI, *Le frodi informatiche*, in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime*, *cit.*, p. 831-834; VITALE, *Brevi riflessioni sul reato di "frode informatica": i servizi a contenuto applicati dalle compagnie telefoniche nell'alveo dei cybercrime*, in *Archivio Penale* n. 1/2015, p. 4 ss..

[421] In questo senso BARTOLI, *La frode informatica tra "modellistica", diritto vigente, diritto vivente e prospettive di riforma,* in *Dir. inf.*, 3/2011, 3, *p. 389,* per cui la fattispecie replicherebbe sia elementi del furto sia della truffa. La giurisprudenza maggioritaria ritiene, invece, che "*il reato di frode informatica (art. 640 ter c.p.) ha la medesima struttura e quindi i medesimi elementi costitutivi della truffa, dalla quale si differenzia solamente perché l'attività fraudolenta dell'agente investe non la persona (soggetto passivo), di cui difetta l'induzione in errore, bensì il sistema informatico di pertinenza della medesima, attraverso la manipolazione di detto sistema. Anche la frode informatica si consuma, pertanto, nel momento in cui l'agente consegue l'ingiusto profitto con correlativo danno patrimoniale altrui (Sez. 6, n. 3065 del 04/10/1999 - dep. 14/12/1999, P.m. e De Vecchis F, Rv. 214942; Sez. 1, n. 36359 del 20/05/2016 - dep. 01/09/2016, Confl. comp. in proc. Vizcaino, Rv. 268252)*". In questi termini Cass. pen. Sez. II, 17-03-2020, n. 10354 consultabile alla banca dati on line *www.pluris-cedam.utetgiuridica.it.*

[422] SCOPINARO, *Internet e reati contro il patrimonio*, *cit.*, p. 47, pur assimilando la frode informatica al furto aggravato dall'uso del mezzo fraudolento, ritiene corretta la previsione del duplice evento di danno-profitto.

attuati[423]- hanno un'incidenza diretta sul sistema o sui dati, che è espressione, in ogni caso, delle facoltà e dei poteri dispositivi della vittima[424]. La fraudolenza passa, cioè, comunque dalla cooperazione "artificiosa" con quest'ultima ma nei modi in cui è resa possibile dall'automazione, su cui ricade la carica decettiva che comporta poi il trasferimento o l'attribuzione indebita.

In questo senso rileva anche la clausola "*senza diritto*" che è riferita all'intervento. In proposito si sono riproposte in dottrina le critiche generalmente mosse a questo tipo di espressioni, che vengono per lo più ritenute superflue perché concepite come sinonimiche dell'arbitrarietà dell'intervento[425]. In realtà, una lettura di questo tipo ne sottovaluta le potenzialità delimitative: come per il delitto d'indebito utilizzo e per quello di accesso abusivo, la locuzione va intesa come inclusiva di un'operatività sia non autorizzata, sia contraria ai parametri normativi-pattizi[426] che definiscono le possibilità d'interazione sia sul sistema, sia a maggior ragione sui suoi contenuti.

Si deve, cioè, trattare del "*tradimento*" oggettivamente verificabile "*delle finalità per le quali si dispone di una qualche potenzialità (di fatto o di diritto)*"[427] di intervento sul sistema: deve sussistere una deviazione, a profitto proprio e danno altrui, dalla regolamentazione dei rapporti che è fissata nell'automazione resa possibile dalle TIC.

Diversamente dall'indebito utilizzo, che è costruito sull'impiego in sé dello strumento di pagamento, il quale in mancanza di profili di delegittimazione sarebbe materialmente corrispondente alla condotta lecita, la frode informatica è incentrata sull'interferenza/interazione fraudolenta con il sistema o con i dati. Conferme in questo senso derivano proprio dalla direzione stessa dell'abusività, che- in armonia alla diversità modale dei delitti- attiene nel caso dell'utilizzo ai limiti di attribuzione derivanti dalla regolamentazione dei rapporti tra titolare dello strumento e terzo, mentre nella frode riguarda la selezione delle attività realizzabili direttamente sui contenuti pertinenti al sistema.

---

[423] In senso critico sulla configurazione sulla base delle predette formulazioni ampie del delitto di frode informatica come reato a forma libera vedi BARTOLI, *op. ult. cit.*.

[424] Cfr. PICOTTI, *Reati Informatici, cit.*, p. 7.

[425] Per l'analisi di questi orientamenti dottrinali si rinvia a C. PECORELLA, *art. 640 ter c.p.*, in DOLCINI-GATTA (a cura di), *Codice Penale Commentato*, *cit.*, p. 1141 ss..

[426] FALCINELLI, *L'abuso del diritto in cerca di direzione penale Spunti dall'esegesi delle Sezioni unite sul delitto di mantenimento abusivo in sistema informatico*, nota a Sez. Un.,18 maggio 2017 n. 41210 relativa all'ipotesi aggravata di cui all'art. 615-ter, c. 2, n. 1) c.p., in *Archivio penale*, 3/2017, p. 11, concepisce il concetto giuridico della abusività come contrasto sostanziale "*ai generali canoni giuridici normativi. In campo penale ciò equivale ad identificare quello che per il senso (di giustizia) collettivo, riflesso nella norma, risulta privo di un valore oggettivo, quindi da non consentire. V'è l'eco delle "finalità ontologicamente diverse" da quelle formalmente assegnate all'agente incaricato, che nello scorrere della riflessione diventano – secondo una ipotesi da verificare – criteri di impunità della vicenda per carenza di reale offensività*". *Contra* LARINNI, *Garantismo europeista: un ossimoro? A proposito dell'accesso abusivo ad un sistema informatico o telematico (615 ter c.p.)*, in www.discrimen.it del 29 giugno 2020, p. 25, che discorre, invece, di ammissione dello sviamento del potere quale tradimento della concezione oggettiva dell'abusività proposta dalla Sezioni Unite. Optano per una soluzione intermedia CASELLATO, DI MAIO, MUSCATELLA, *Il nodo gordiano dello "sviamento di potere" nell'accesso abusivo ad un sistema informatico, tra suggestioni dogmatiche e riflessioni giurisprudenziali*, in *Cass. pen.*, 7/2019, p. 2790.

[427] Così FUMO, *La condotta nei reati informatici*, in *Archivio Penale*, 3/2013, p. 791.

Ne deriva, pertanto, che anche laddove lo strumento di pagamento impiegato fosse clonato o contraffatto, non si potrebbe *ex plano* affermare la sussistenza della frode informatica in assenza di quell'interfaccia vietata con il sistema, da cui derivi la disposizione produttiva del duplice evento di ingiusto profitto con altrui danno.

Una ricostruzione di questo tipo è sostanzialmente coerente con il contenuto dell'obbligo d'incriminazione della frode connessa ai sistemi di informazione di cui all'art. 6 della direttiva 713/2019.

Premesso che conformemente alle previsioni della Convenzione Cybercrime, il legislatore sovranazionale reputa sufficiente il dolo specifico di profitto[428], sulla base del tenore letterale del citato articolo 6 non sembra si possa dubitare che l'"*atto di effettuare o indurre un trasferimento di denaro, valore monetario o di valuta virtuale arrecando illecitamente a terzi una perdita patrimoniale allo scopo di procurare un ingiusto profitto all'autore del reato o a una terza parte*" costituisca il risultato materiale della condotta di frode, che coincide o da cui dovrebbe conseguire l'evento di danno[429].

In apparente conformità a questo obbligo d'incriminazione, lo schema del decreto legislativo di attuazione della direttiva UE/2019/713 contempla l'introduzione, all'art. 640 ter c.p., 2 comma, della previsione di una circostanza aggravante di "produzione" di un trasferimento di denaro, di valore monetario o di valuta virtuale[430].

Come riferito, questa circostanza aggravante è giustificata essenzialmente da ragioni di "allineamento sanzionatorio"[431] della frode al regime sanzionatorio dell'art. 493 ter c.p.

Questa operazione genera diversi dubbi, a partire dalla sua doverosità in conformità a quel giudizio di disvalore che è riferibile al legislatore sovranazionale.

---

[428] Per PICOTTI, *Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale, cit.*, p. 201, per cui "*Un siffatto arretramento della soglia di punibilità appare conforme alla formulazione del reato comune di truffa presente in altri ordinamenti (quali la Francia, la Germania, la Spagna): ma rappresenterebbe, per il nostro, una deviazione dallo schema tradizionale delineato dall'art. 640 c.p., cui il legislatore del 1993 ha voluto attenersi, caratterizzato da tale "doppio" evento consumativo. Eppure l'accoglimento delle indicazioni contenute nella norma internazionale potrebbero rappresentare una razionalizzazione della nostra disciplina in materia, perché mentre il fine specifico sarebbe comunque indicativo del "conflitto di interessi" che deve stare alla base dell'incriminazione delittuosa, si eviterebbero ingiustificati scivolamenti del momento consumativo o, comunque, difficoltà di prova dell'evento ulteriore, spesso dedotto solo per presunzioni, che non sembra particolarmente significativo sul piano dell'offesa oggettiva*".

[429] Una ricostruzione di questo tipo può essere avvalorata da una lettura integrata della disposizione in esame con quella antecedente portata dalla Convenzione di Budapest e di cui la direttiva 713 sembra replicare la struttura. Nello specifico l'art. 8 della Convenzione riferisce la frode informatica alla commissione intenzionale e senza alcun diritto del cagionare un danno patrimoniale ad altra persona mediante "a. *ogni introduzione, alterazione, cancellazione o soppressione di dati informatici; b. con ogni interferenza nel funzionamento di un sistema informatico, con l'intento fraudolento o illegale di procurare, senza alcun diritto, un beneficio economico per se stesso o altri*".

[430] Vedi la nota 262 per la consultazione del testo del secondo comma dell'art. 640 ter c.p. integrato con le modifiche indicate dallo schema di decreto in esame.

[431] Si rinvia in proposito alla nota 263.

Nello specifico, l'art. 9 della direttiva UE/2019/713 stabilisce, in riferimento all'obbligo d'incriminazione di condotte corrispondenti al delitto nazionale di frode informatica, livelli edittali superiori a quelli indicati per le modalità da incriminare corrispondenti ai delitti nazionali puniti dall'art. 493 ter c.p.[432].

Se il legislatore nazionale avesse voluto effettivamente operare una conforme operazione di allineamento sanzionatorio, avrebbe dovuto farlo in termini praticamente inversi, non certo optando per una circostanza aggravante come quella in esame, la quale risulta non solo ingiustificata, ma anche superflua.

Si rammenta, infatti, che un trasferimento di utilità economicamente rilevante, analogo a quello di cui alla predetta circostanza aggravante, è di per sé implicito[433] nella struttura della fattispecie nazionale di frode informatica; appare anzi possibile ritenere che sia proprio questo requisito, quale causativo di ingiusto profitto con altrui danno, a garantire sul piano dell'offesa la permanenza di una connotazione "patrimoniale"[434].

Elevarlo a fattore aggravante rischia, pertanto, di rendere dubbia l'identità complessiva di questo delitto, che appare di per sé riferibile- in via principale e non meramente strumentale- alla tutela del regolare funzionamento dei sistemi informatici[435].

---

[432] Per una migliore comprensione si riporta di seguito il testo dell'art. 9 della direttiva UE/2019/713: "*Gli Stati membri adottano le misure necessarie affinché i reati di cui agli articoli da 3 a 8 siano punibili con sanzioni penali effettive, proporzionate e dissuasive. Gli Stati membri adottano le misure necessarie affinché i reati di cui all'articolo 3, all'articolo 4, lettere a) e b), all'articolo 5, lettere a) e b), siano punibili con una pena detentiva massima non inferiore a due anni. Gli Stati membri adottano le misure necessarie affinché i reati di cui all'articolo 4, lettere c) e d), e all'articolo 5, lettere c) e d), siano punibili con una pena detentiva massima non inferiore a un anno. Gli Stati membri adottano le misure necessarie affinché i reati di cui all'articolo 6 siano punibili con una pena detentiva massima non inferiore a tre anni. Gli Stati membri adottano le misure necessarie affinché i reati di cui all'articolo 7 siano punibili con una pena detentiva massima non inferiore a due anni. Gli Stati membri adottano le misure necessarie affinché i reati di cui agli articoli da 3 a 6 siano punibili con una pena detentiva massima non inferiore a cinque anni, qualora siano commessi nell'ambito di un'organizzazione criminale quale definita nella decisione quadro 2008/841/GAI, indipendentemente dalla sanzione ivi prevista*".

[433] MUCCIARELLI, *Commento all'art. 10 della l. 23/12/1993 n. 547*, in *Legislazione Penale*, 1996, p. 138, che ravvisa nella fattispecie di frode informatica un "*elemento costitutivo inespresso, rappresentato dalla disposizione patrimoniale (produttiva del vantaggio con altrui danno) che viene posta in essere dal sistema informatico o telematico, a ciò abilitato, in conseguenza della alterazione o dell'intervento abusivo previa mente realizzato dall'agente*".

[434] In questo senso MINICUCCI, *Le frodi informatiche*, in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime*, *cit.*, p. 837 per cui in relazione al danno, vi sarebbe "*un triplice ordine di ragioni che impone di prescegliere la concezione "economico-patrimoniale" (…) In particolare: a) non solo, e non tanto, perché è l'unica a far salva la natura di reato di evento della frode informatica (e della truffa semplice), che senza una apprezzabile consistenza patrimoniale a costituire il riferimento ultimo dell'illecito vedrebbero altrimenti la loro inesorabile metamorfosi in illeciti di pericolo; b) perché lo snaturamento del profilo patrimonialistico del danno sarebbe in rotta di collisione, appunto, con il bene giuridico protetto, finendo col generare una sovrapposizione concettuale con le varie forme di danneggiamento informatico ex artt. 635-bis ss.; c) perché, anche con riferimento all'art. 615-quater c.p., si genererebbe una identica confusione, laddove si ammettesse che il profitto derivi semplicemente a seguito del fatto (e non a sua causa), oppure che lo stesso abbia una natura non marcatamente economico-patrimoniale*".

[435] Così, pur affermando la natura plurioffensiva del reato, MEZZETTI, *Reati contro il patrimonio*, in GROSSO-PADOVANI-PAGLIARO (diretto da), *Trattato di diritto penale. Parte speciale*, XV, Milano, 2013, p. 461.

In questo senso depone, peraltro, la stessa selezione delle condotte punibili, anche nel raffronto con quelle oggetto dell'obbligo d'incriminazione.

Nello specifico, sulla base dell'art. 6 citato, è richiesto agli Stati membri di punire l'ostacolo/interferenza sul funzionamento del sistema e l'introduzione, l'alterazione, la cancellazione, la trasmissione o la soppressione di dati, realizzate in entrambi i casi "senza diritto" e con il fine d'ingiusto profitto. La prima tipologia di condotte è sostanzialmente coincidente con quella nazionale di alterazione, che non è connotata dal carattere indebito, invece previsto per l'altra modalità di condotta, relativa ai dati. Quest'ultima è descritta, in conseguenza del riferimento all'intervento, in maniera più estesa rispetto all'elencazione sovranazionale: si tratta, infatti, di espressione che sembra rimandare, più che ad un'attività manipolativa[436], a quella generale di trattamento dei dati.

Questa scelta normativa è apprezzabile se si considera che la centralità assunta dal dato informatico, alla luce della variabilità di contenuti e funzioni che può avere, abbia comportato che alla "*Computer Security, ossia protezione del computer o, più in generale, del sistema informatico, dei suoi apparati, dei programmi informatici e delle infrastrutture*" sia stata "*progressivamente affiancata e integrata da una visione della sicurezza maggiormente orientata alla protezione delle informazioni e dei dati, la c.d. Information Security*"[437].

Entrambi questi profili possono essere certamente ricondotti alla *cybersecurity*, quale sintesi assiologica che le abbraccia entrambe e che è certamente sottesa alla prospettiva di tutela della sicurezza del mercato digitale, su cui sono stati costruiti gli obblighi d'incriminazione portati dalla direttiva UE/2019/713.

Come già rappresentato[438], l'atto sovranazionale richiama, in funzione integrativa definitoria della dimensione fattuale di riferimento e dei corrispondenti contenuti degli obblighi d'incriminazione, la direttiva 2013/40/UE e la direttiva 2016/1148/UE, aderendo in questo modo implicitamente ad una concezione di sicurezza informatica quale "*capacità di una rete e dei sistemi informativi di resistere*

---

[436] In questo senso C. PECORELLA, *Diritto penale dell'informatica*, II ed., Padova, 2006, p. 90 ss.; *Contra* PICOTTI, *op. ult. cit.*, il quale evidenzia come il reato copra, invece, anche profili propri di una figura d'infedeltà patrimoniale. Tra gli Autori ha ricondotto -in opposizione all'alterazione- l'intervento senza diritto ad una modificazione intrinseca e condizionante le singole istruzioni impartite al sistema PARODI, *La frode informatica: presente e futuro delle applicazioni criminali nell'uso del software*, in *Diritto penale e processo, 12*/1997, p. 1538, il quale richiama come ipotesi riferibile alla condotta di alterazione quella di danneggiamento, mentre costituirebbe un intervento senza diritto uno spostamento di denaro attuato indebitamente mediante i servizi telematici degli istituti di credito.

[437] BRIGHI, *Cybersecurity. Dimensione pubblica e privata della sicurezza dei dati*, in CASADEI, PIETROPAOLI (a cura di), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Cedam, 2021, p. 135.

[438] Si rinvia alle note 193 e 194.

(…)a ogni azione che comprometta la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati o trasmessi o trattati e dei relativi servizi offerti o accessibili tramite tale rete o sistemi informativi"[439].

3.4 Questioni problematiche irrisolte

Con lo schema del decreto legislativo di attuazione della direttiva UE/2019/713 non sono state in generale considerate le caratteristiche tecniche peculiari che caratterizzano la conservazione e il trasferimento di valute virtuali.

Si ribadisce, infatti, che il loro scambio è l'esito di comunicazione criptate decifrate mediante le chiavi privati.

In considerazione di quanto sopra, l'individuazione delle fattispecie applicabili all'acquisizione ed operatività illecita in valute virtuali è questione che va oltre la definizione dei rapporti tra il delitto di frode informatica e quello d'indebito utilizzo di cui all'art. 493 ter c.p..

Ma guardando alla frode informatica, non sembra sussistere dubbio sulla sussistenza di questo delitto nei casi in cui il conseguimento della disponibilità delle valute virtuali avvenga mediante attacchi *hacker*[440] al sistemo informatico del singolo o del *Virtual asset service provider*[441], anche attraverso tecniche di *phishing* che rendano possibili le c.d. *wallet address scams*[442], o ancora ai sistemi di *mining pool*[443].

Anzi, attacchi di questo tipo che siano rivolti ai *wallet providers* o agli *exchanges* o anche alle piattaforme di *trading* pongono la differente questione dell'introduzione di profili di responsabilità, anche penali, che potrebbero derivare da una previa imposizione a loro carico di obblighi a garanzia di standard di sicurezza informatica conformi alla rilevanza degli interessi in gioco.

Tralasciando momentaneamente questo aspetto, che involge regimi di responsabilità anche di enti collettivi in funzione di prevenzione, nell'emendamento del delitto di frode informatica andava in ogni caso valutata la possibilità di considerare la chiave privata quale elemento che integra l'ipotesi aggravata dal "*furto o indebito utilizzo dell'identità digitale in danno di uno o più soggetti*" [444].

---

[439] Così art. 4 della direttiva 2016/1148/UE.

[440] BONCOMPAGNI, *Crimini informatici e criptovalute*, in CAPACCIOLI, *Criptoattività, criptovalute e bitcoin*, *cit.*, p. 304.

[441] Sulla definizione di questa peculiare tipologia di provider vedi la nota 136.

[442] Sul punto diffusamente le note da 109 a 112.

[443] BONCOMPAGNI, *Crimini informatici e criptovalute*, in CAPACCIOLI, *Criptoattività, criptovalute e bitcoin*, *cit.*, p. 305, precisa che si tratta di attacchi all'aggregazione dei sistemi che uniscono i poteri di *hashing* per minare criptovalute, in cui l'hacker mediante codici dannosi si appropria delle chiavi private dei miners o modifica gli indirizzi della *mining pool* in modo che le criptovalute siano direttamente minate in suo favore.

[444] Sulle considerazione svolte sul contenuto e sull'introduzione di questa aggravante al 3 comma dell'art. 640 ter c.p. vedi il paragrafo 2.1.

Si tratta di un'aggravante che avrebbe dovuto inasprire il contrasto al *phishing*, ma che ha destato critiche in dottrina[445], richiedendo, pur nella sua formulazione ambigua[446], lo "sfruttamento" illecito dell'identità altrui, quale strumento per operare fraudolentemente sul sistema o sui dati in esso contenuti[447].

In assenza di una definizione ai fini penali dell'identità digitale, sono state ad essa ricondotte le credenziali di accesso a un sistema informatico, quali *username* e *password*, o anche informazioni biometriche[448].

In realtà, in considerazione della strumentalità segnalata, va preferita la corrispondenza, prospettata da autorevole dottrina, del concetto d'identità digitale a "*dati e informazioni di autenticazione o di abilitazione che afferiscono ad un'ampia area di riservatezza del titolare*"[449], piuttosto che a profili d'identificazione dell'utente informatico.

---

[445] In questo senso DI PAOLO, *Cyber crime. Il Phishing: prospettive di un delitto*, in *Archivio penale, 2/ 2017,* p. *19* secondo cui "*ritenere che il phisher risponda dei reati di accesso abusivo e di frode informatica, seppure nella forma aggravata perché commessa con furto di identità digitale, non sembra cogliere tutte le sfumature cromatiche del Phishing, nel suo concreto dispiegarsi*". Per l'esame dell'applicazione giurisprudenziale di questo istituto si rinvia a Cass. pen., sez. II, sentenza 24.10.2018 n. 48553, con nota di SCARCELLA, *Il phishing è punibile come frode informatica*, in *Quotidiano Giuridico* del 13.11.2018, per cui "*integra il reato di frode informatica la condotta consistente nell'accesso abusivo a conti correnti on line cui segua il prelievo di somme fatte confluire su carte prepagate appositamente attivate a tal scopo a nome e da persone in condizioni economiche disagiate, materialmente estranee all'accesso abusivo, in cambio di un compenso legato al solo fatto della apertura del rapporto sottostante il rilascio della carta prepagata*."

[446] In questi termini CAJANI, *La frode informatica*, in PARODI (a cura di), *Diritto penale dell'impresa*, Giuffrè, 2017, p. 565, si esprime, comunque, per un giudizio complessivamente positivo, anche in considerazione della maggiore carica di ambiguità che, a suo dire, sarebbe stata riferibile alla formulazione di "*sostituzione dell'identità digitale*", utilizzata nella versione precedente alla conversione in legge del d.l. n. 93/2013. In generale, sull'idoneità dell'espressione "*furto d'identità digitale*" vedi ZICCARDI, *Furto d'identità,* in *Digesto pen*., VI, agg., Torino, 2001, p. 253-254, che contesta l'impiego sia del termine furto, a cui sarebbero da preferire espressioni come "*clonazione, impersonificazione o frode*", sia di quello identità, potendo essere carpiti solo alcuni dati rilevanti riferibili a questa, come quelli bancari, medici, numeri di carte di credito, altri dati sensibili d'interesse del criminale.

[447] Vi attribuisce una valenza più ampia, assorbente il delitto di sostituzione di persona CAJANI, *La tutela penale dell'identità digitale alla luce delle novità introdotte dal d.l. 14 agosto 2013 n. 93 (convertito con modificazioni dalla l. 15 ottobre 2013, n. 119)*, in *Cass. pen*., 3/2014, p. 1096 per cui "*pur riconoscendosi in astratto una non perfetta sovrapponibilità tra la condotta di chi «sostituisca illegittimamente la propria all'altrui persona, o attribuisca sé o ad altri un falso nome, o un falso stato, ovvero una qualità a cui la legge attribuisce effetti giuridici» e quella di chi «rubi o indebitamente utilizzi una identità digitale con altrui danno», pare forse più correttamente sostenibile – nella maggior parte dei casi concretamente ipotizzabili – la tesi di un concorso formale tra reati, attribuendo così la natura di reato complesso alla nuova previsione dell'art. 640-ter comma 3 c.p.*"; *contra* FLOR, *Phishing e profili penali dell'attività illecita di "intermediazione" del cd. Financial manager*, *cit*., p. 60.

[448]Si rinvia per una completa sintesi delle diverse posizioni adottate in dottrina a FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative,* in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime*, *cit*., p. 169-171, per cui "*in ogni caso, pur tentando con estrema difficoltà, con riferimento alle condotte tipiche, di fornire soluzioni interpretative nei limiti imposti dal divieto di estensione analogica in malam partem, rimane irrisolto il problema definitorio dell'«identità digitale», che come già è emerso sopra, potrebbe essere intesa, da un lato, in senso restrittivo, ossia quale "profilo abilitativo" o "credenziali di autenticazione" ; dall'altro lato, potrebbe essere ricondotta nell'ambito del più complesso sistema di protezione dei "dati personali""*.

[449] Testualmente FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative,* in CADOPPI , CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime*, *cit*., p. 171 mette in luce come mediante la predetta aggravante siano stati posti in essere "*tentativi definitori che (..) sembrano ruotare attorno alla c.d. fase autenticativa*

Una valenza di questo tipo può certamente essere riferita alla funzione propria delle chiavi private, rispetto alle quali i predetti profili di riservatezza possono anche riguardare, laddove la sua acquisizione avvenga "in itinere", quella delle comunicazioni informatiche criptate, mediante le quali è effettuato lo scambio di criptovalute.

A conferma della bontà di questa ricostruzione, consona alle peculiarità tecniche di riferimento, si è già rappresentato come nella relazione di accompagnamento dello schema del decreto legislativo di attuazione della direttiva UE/2019/713 siano state indicate come condotte mediante le quali conseguire l'ottenimento illecito di strumenti di pagamento immateriale, oltre al delitto di accesso abusivo ad un sistema informatico o telematico, anche quelle di intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche, nonché di falsificazione, alterazione o soppressione del loro contenuto, punite dagli artt. 617 quater e 617 sexies c.p.[450].

3.5 Questioni problematiche future.

Nonostante queste "indicazioni", lo schema del decreto legislativo di attuazione della direttiva UE/2019/713 prevede l'introduzione, mediante inserimento nel codice penale dell'art. 493 quater, di un nuovo delitto di detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti, che, come riferito, desta dubbi a partire dall'individuazione di questi reati-fine.

Sulla falsariga dell'art. 615 quinquies c.p., che è reato prodromico ai delitti di danneggiamenti informatici[451], le modalità della condotta di questo proposto nuovo delitto sono descritte in maniera

– piuttosto che a quella riconoscitiva – collegata a condotte di "furto" d'identità digitale, in cui il fulcro del disvalore sociale è incentrato sulla acquisizione o sulla sottrazione dei dati riservati".

[450] Si rinvia alla nota 244.

[451] In questo senso espliciti sono la rubrica della disposizione e il contenuto del dolo specifico; con riferimento all'elemento soggettivo PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, *cit*., p. 710, rappresenta come "*l'attuale fattispecie del codice italiano finisce per tipizzare condotte in sé perfettamente lecite, dal punto di vista oggettivo, ed anzi usuali nell'attività di ogni operatore commerciale o privato ("procurarsi, produrre, riprodurre, importare, diffondere, comunicare, consegnare, mettere a disposizione di altri"), riferite ad "apparecchiature, dispositivi e programmi informatici" a loro volta non connotati in alcun modo come in sé dannosi o pericolosi. È solo il fine dell'agente (c.d. dolo specifico) che rende penalmente illecito il fatto*". In termini analoghi anche RESTA, *Cybercrime e cooperazione internazionale, nell'ultima legge della legislatura,* in *Giur. merito*, fasc.9/2008, p. 2147 ss..

abbastanza ampia[452] e distinguibili fra quelle di acquisizione in proprio favore e quelle di distribuzione a terzi[453] di questi peculiari mezzi.

Quest'ultimi, sono descritti come "*apparecchiature, dispositivi o programmi informatici progettati al fine principale*" di farne uso o di consentire ad altri di farne uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti o "*specificamente adattati al medesimo scopo*".

Come risulta dalla relazione di accompagnamento, la peculiare qualificazione dell'oggetto del reato, unitamente alla previsione del dolo specifico, concentra "*il disvalore penale sui casi in cui il dato materiale sia precisamente illuminato dalla finalità soggettiva e viceversa, in cui cioè alla finalità soggettiva si affianchi una qualche materialità della condotta*"[454]. Conformemente alla soluzione di compromesso che era stata adottata già dalla Convenzione di Budapest[455], il fattore di prevalenza o di specificità della funzionalità "illecita" del mezzo è riferito alla progettazione o al suo adattamento al perseguimento di essa.

Nonostante possa generare dubbi sul piano della determinatezza, questa strutturazione garantisce, comunque, rispetto alla previsione espressa di un requisito di "idoneità" del mezzo, un livello di "elasticità" compatibile con una legittima normazione in ambito penale.

Se quindi sul piano della connotazione illecita del mezzo lo sforzo legislativo è apprezzabile, non lo è sul piano dell'individuazione della sua tipologia.

L'art. 493 quater previsto dallo schema del decreto in esame, non introducendo ai fini dell'identificazione dell'oggetto materiale del reato nemmeno il riferimento ai dati informatici, delinea, infatti, una fattispecie "eccentrica" rispetto alla possibile fenomenologia di base e destinata solo a creare dubbi di sovrapposizione con i reati prodromici ai delitti informatici di ottenimento illecito degli strumenti di pagamento immateriali.

---

[452]Può risultare inopportuna solo l'omessa previsione della "riproduzione", data la riproducibilità che connota i programmi informatici. In questi termini con riferimento alla formulazione delle modalità della condotta incriminata dall'art. 615 quinques c.p., ante legge 48/2008, vedi PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, cit., p. 709

[453] Le tipologie di condotte incriminate dal neo delitto risultano sostanzialmente simile a quella prevista dall'art. 615 quinques c.p. nella formulazione emendata dalla l. n. 48/2008, di ratifica ed esecuzione della Convenzione Cybercrime. Per una disamina del delitto, previsto da questo articolo, di diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico vedi SALVADORI, *I reati contro la riservatezza informatica*, in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime*, *cit*., p. 702, il quale distingue essenzialmente due categorie di condotte, quelle volte a "far entrare" nella sfera altrui questi oggetti e quelle dirette a farli entrare nella sfera di signoria dell'agente.

[454] Testualmente la relazione illustrativa, *op. ult. cit.*.

[455] In questo senso PICOTTI, *Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale, cit.*, p. 200, che definisce la scelta della Convenzione sul punto "*una via di mezzo fra le due possibilità estreme di incriminare soltanto dispositivi di per sé illeciti e come tali concepiti fin dall'origine; ovvero qualsiasi dispositivo utilizzabile, di fatto, anche per fini non leciti. Secondo il rapporto esplicativo, in quest'ultima ipotesi si sarebbe corso il rischio di un penalizzazione eccessiva, che avrebbe potuto estendersi ad ogni dispositivo "a doppio uso" (lecito ed illecito), come sono quelli per testare la sicurezza di un sistema o l'affidabilità dei prodotti, o per l'analisi di una rete. Mentre la loro esclusione avrebbe ristretto troppo la portata dell'incriminazione*".

Come già rappresentato, il difetto di selezione emerge nel raffronto con il menzionato delitto di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici, di cui all'art. 615 quater c.p., potendo effettivamente le chiavi private, nelle differenti forme di archiviazione rese possibili da wallet on line ed off line[456], costituire "*codici, parole chiave o altro mezzo idoneo all'accesso ad un sistema informatico o telematico*"[457].

Sempre con riferimento a questo delitto si pone quale ulteriore fattore differenziale il contenuto del dolo specifico, che nel caso dell'art. 615 quater c.p. è costituito dal fine di profitto o di arrecare ad altri un danno[458], mentre nel proposto art. 493 quater è indicato nel fine di farne uso o di consentire ad altri di farne uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti.

Questo peculiare contenuto del fine tipico, se letto unitamente alle modalità della condotta, in realtà crea importanti momenti di "frizione" anche con l'art. 617 quinquies c.p., il quale è reato prodromico all'intercettazione o all'impedimento delle comunicazioni tra sistemi informatici che si consuma nel momento effettivo dell'istallazione[459] di apparecchiatura "*atta ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi*".

Si tratta di reato di pericolo concreto[460], rispetto al quale l'art. 493 quater portato dalla schema del decreto sembra destinato a generare un'ulteriore anticipazione dell'intervento penale, ancorché limitata alle ipotesi riferibili agli strumenti di pagamento diversi dai contanti.

---

[456] Si rinvia in proposito alla nota 105.

[457] Per SALVADORI, *I reati contro la riservatezza informatica*, in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime*, *cit*., p. 697, definisce il contenuto delle modalità di condotta dell'art. 615 quater c.p. nei seguenti termini: "*per «codice» o «parola chiave» deve intendersi qualsiasi sequenza alfanumerica (o password) idonea a consentire a chi ne ha la disponibilità di accedere ad un sistema informatico protetto da misure di sicurezza116. Mediante la locuzione «altri mezzi idonei», che si configura quale "clausola di chiusura" estremamente elastica, capace di ricomprendere anche gli strumenti tecnologici non ancora scoperti, il legislatore ha voluto sanzionare non solo i software multifunzionali o multiscopo che consentono di aggirare le misure di sicurezza poste a protezione di un sistema informatico e di accedere ai dati ed ai programmi in esso contenuti (c.d. hacking tools), ma anche qualsiasi dispositivo o mezzo fisico (ad es. una tessera magnetica), che permetta di introdursi in un sistema*".

[458] SALVADORI, *I reati contro la riservatezza informatica*, in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime*, *cit*., p. 699, sostiene che "*con l'opportuna previsione del dolo specifico, il legislatore abbia voluto limitare la punibilità ai comportamenti, prodromici e preparatori alla commissione di un reato informatico, in quanto commessi dall'agente al fine di procurarsi un profitto ovvero di arrecare ad altri un danno e che, di conseguenza, si pongono in oggettivo contrasto con gli interessi giuridici (alla riservatezza informatica ed alla esclusiva disponibilità ed integrità dei dati e dei sistemi informatici) altrui, tutelati dalla norma incriminatrice*".

[459] C. PECORELLA, *sub art. 617 quinques c.p.*, *cit*., p. 2148.

[460] Così SALVADORI, *I reati contro la riservatezza informatica*, in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime*, *cit*., p. 714, per cui "*tali apparecchiature devono essere oggettivamente idonee («atte ad intercettare») a produrre l'evento lesivo, vale a dire ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche. Tale idoneità deve essere accertata in concreto da parte del giudice*"; C. PECORELLA, *sub art. 617 quinques c.p.*, *cit*., p. 2149, da atto di sentenze che hanno svuotato di significato la lettera della norma, ritenendo sufficiente una mera idoneità in astratto.

In realtà, l'effetto limitativo è solo apparente, perché la peculiarità di questi strumenti non incide, mutandola, sull'oggettività fattuale ed offensiva di riferimento delle condotte prodromiche alla realizzazione dei delitti di intercettazione, nonché di quelli di accesso abusivo o di frode informatica. Rispetto a conseguenze problematiche di tal fatta, si coglie l'inadeguatezza d'interventi settoriali, che non solo non sono all'altezza della rilevanza della cornice di "sicurezza del mercato digitale" in cui essi si iscrivono, ma non riescono nemmeno a coglierne la valenza sistematica.

Il cyberspace costituisce oggi una nuova realtà sociale che si sovrappone e condiziona quella materiale[461]; il ricorso in generale a strumenti e mezzi digitali fa emergere bisogni di tutela propri, ma la cui garanzia è funzionale anche al fisiologico sviluppo delle transazioni economiche in genere, che avvengono anche loro tramite[462].

La novità di queste commistioni sta nel fatto che la tutela d'interessi individuali, come quelli patrimoniali, è dipendente dall'interazione delle regole giuridiche con quelle tecniche che governano le strutture informatiche[463] ed il cui rispetto è necessario per il loro stesso corretto funzionamento.

L'ottenimento illecito degli strumenti di pagamento immateriali realizzabile mediante reati informatici non patrimoniali, che dovrebbero essere a tutela della riservatezza, o ancora di reati informatici patrimoniali, ma "indirizzati" verso altri momenti di tutela, dimostra come la conformazione digitale del mezzo o del contesto di scambio abbia una valenza "prevalente".

Ne consegue che eventuali interventi di contrasto delle frodi e delle falsificazioni degli strumenti di pagamento diversi dai contanti avrebbero dovuto essere concepiti come interessanti direttamente i sistemi, gli spazi e le comunicazioni informatiche che le rendono possibili, in una logica di "strumentalità" inversa.

---

461 BRIGHI, *La vulnerabilità nel cyberspazio*, in *Ars interpretandi*, 1/2017, p. 82-83 per cui "*Alle tradizionali funzioni epistemiche, dove i computer con i processi di elaborazione dell'informazione estendono le capacità cognitive dell'uomo (calcolare, pianificare, ricordare, ricercare ecc.), con i processi di creazione di ambienti e di oggetti virtuali che estendono il mondo fisico, si aggiunge, di fatto, una funzione ontologica*". Discorre, invece, di "terzo spazio", definito "*come l'ambiente naturale e sociale, la rete si connota come un contesto regolato da norme peculiari, attraversato da dinamiche specifiche, caratterizzato da conflitti peculiari, che sfociano nella produzione di rappresentazioni e identità del tutto inaspettate*", SCALIA, *Relazioni pericolose nel "terzo spazio"*, in *Diritto Penale Uomo*, 1/2021, p. 110.

462 Cfr. PICOTTI, *Cybersecurity: quid novi?*, *cit.*, p. 11, rileva come dagli anni Ottanta, "*parallelamente all'informatizzazione di settori sempre più importanti dell'economia e della pubblica amministrazione*", la tutela della sicurezza informatica fosse vista "*come strumentale alla tutela di altri beni giuridici "finali", sia della persona, sia della collettività*".

463 PICOTTI, *Sicurezza, informatica e diritto penale*, In DONINI-PAVARINI (a cura di), *Sicurezza e Diritto penale*, 2011, p. 243, nel considerare la predetta interazione mette in luce come "*le "regole" e le misure tecniche proprie dell'automazione" dovrebbero "rappresentare lo strumento efficace di rafforzamento e garanzia della disciplina giuridica, per la loro funzione intrinsecamente preventiva, che può consentire al diritto penale di svolgere quel ruolo sussidiario di extrema ratio, che gli compete*".

Capitolo V

Considerazioni conclusive nella prospettiva della sicurezza informatica

Sommario: 1. La tutela del patrimonio digitale attraverso la sicurezza informatica; 2.Considerazioni di stile; 3. *Locus commissi delicti* e *locus* "informatico"; 4. Verso profili procedurali di responsabilità a garanzia della sicurezza informatica.

1. La tutela del patrimonio digitale attraverso la sicurezza informatica.

Tirando le somme della ricerca svolta, si può innanzitutto affermare che le forme di aggressione alle manifestazioni di quella che potrebbe essere definita come "ricchezza digitale" non sono sussumibili nelle tradizionali fattispecie contro il patrimonio, data la diversità delle condotte e dei relativi mezzi ed oggetti.

Non è, pertanto, corretto porsi un problema di "revisione" interpretativa di queste fattispecie o di adozione di una concezione evolutiva del concetto di "cosa": nel caso delle valute virtuali e più in generale delle entità digitali che assumono valore di scambio, non sono predicabili gli schemi classici della sottrazione e dell'impossessamento, perché inidonei ad aggredirne le forme di controllo, accessibilità ed esclusività.

La dematerializzazione non determina una modifica radicale del modo d'intendere il patrimonio, ma l'emersione di esigenze di tutela penale ulteriori, direttamente discendenti dalla dimensione digitale che esso assume.

Rispetto a queste nuove esigenze di protezione penale, non basta predicare la logica "cumulativa" della plurioffensività[464].

Non è, infatti, questione di pluralità d'interessi, ma di tutela dell'"*affidabilità e (del)la sicurezza del ricorso alla tecnologia informatica, telematica e cibernetica*"[465], che deve essere garantita quale nuovo bene giuridico, indipendentemente dalla natura degli interessi che possono essere suo tramite soddisfatti.

---

[464] Sulla ricostruzione in questi termini della plurioffensività quale oggetto di tutela unico "*quantunque strutturalmente definito dalla fusione di più interessi*" si rinvia a DURIGATO, *Rilievo sul reato plurioffensivo*, Cedam, Padova, 1972, p. 37.

[465] In questi termini FULVI, *La Convenzione Cybercrime e l'unificazione del diritto penale dell'informatica*, in *Diritto penale e processo* 5/2009, p. 642-643. Per l'Autore l'individuazione di un comune oggetto di tutela alla base del diritto penale dell'informatica consente nella prospettiva di una unificazione categoriale dei reati informatici la considerazione degli altri singoli beni individuali contestualmente offesi, tra cui appunto il patrimonio, come "*marcatori di zona, per graduare la gravità delle fattispecie*". In termini analoghi con riferimento ai reati informatici del codice spagnolo vedi RUEDA MARTÌN, *La confidencialidad, integridad y disponibilidad de los sistemas de información como bien jurídico protegido en los delitos contra los sistemas de información en el código penal español*, in *Diritto penale contemporaneo, Rivista trimestrale*, 3/2020, p. 211, che considera la "*confidencialidad, integridad y disponibilidad de los sistemas informáticos como bien jurídico protegido dotado de autonomía y que, además, sirve de barrera de contención de riesgos para otros bienes jurídicos que puedan verse implicados en la utilización de sistemas y redes informáticos*".

Si tratta, cioè, di quel bene a rilevanza pubblicistica che è stato identificato nella sicurezza informatica[466], nella duplice componente interconnessa ed indistinguibile della *computer security* e della *information security*.

A conferma di come la natura composita di questo bene si rifletta a livello penalistico, può essere richiamata la possibile derivazione, in funzione aggravante di un accesso abusivo, ai sensi del secondo comma dell'art. 615 ter c.p., del reato di danneggiamento informatico[467].

Già a livello di previsione delle fattispecie è, infatti, possibile cogliere quella connessione con la riservatezza informatica[468], che è peraltro sinteticamente rappresentata, a livello di fonti sovranazionali, dalla c.d. "*triade CIA (Confidentiality, integrity, availability)*"[469], in virtù della quale la *cybersecurity* diviene "*garanzia di certezza*"[470] dei rapporti digitali e dei relativi flussi comunicativi.

Per autorevole dottrina, nell'attuale contesto *dell'Internet of Things*, d'interconnessione fisica-virtuale, uomo-sistema informatico ovvero tra sistemi, essa potrebbe essere, addirittura, concepita come "*safety*", quale protezione, cioè, diretta del singolo dai pericoli connessi alla fruizione di sistemi e dati informatici.[471]

Il legame con la riservatezza messo in luce consente, inoltre, di ribadire la dimensione sovraindividuale e di "sistema" che connota la sicurezza informatica, la quale va oltre le categorie penalistiche tradizionali e non è ad avviso di chi scrive considerabile in termini di "bene comune", nemmeno laddove inteso quale "*fascio di beni giuridici ossia aree di tutela funzionalmente unitaria, non*

---

[466] Cfr. PICOTTI, *Sicurezza, informatica e diritto penale*, *cit*., p. 241, il quale nel riconoscerlo come nuovo bene giuridico gli attribuisce una valenza duplice: passiva relativamente allo sbarramento da accessi indebiti e attiva nell'imposizione di apposite procedure tecniche conformi.

[467] Cfr. SALVADORI, *Il " microsistema " normativo concernente i danneggiamenti informatici. Un bilancio molto poco esaltante,* in *Rivista italiana di diritto e procedura penale,* n. 1/2012, p. 238-241, il quale, partendo dalla considerazione che la tutela del patrimonio del proprietario dei dati e sistemi informatici è presente, ma solo sullo sfondo, propone in prospettiva *de iure condendo* l'inserimento di un nuovo titolo del codice sotto il bene di categoria costituito dalla sicurezza informatica e comprensivo di tutti i delitti che offendono, appunto, la riservatezza, l'integrità e la disponibilità di dati e sistemi informatici.

[468] FLOR, *Riservatezza informatica e sicurezza informatica quali nuovi beni giuridici penalmente protetti*, in MILITELLO, SPENA (a cura di), *Mobilità, sicurezza e nuove frontiere tecnologiche*, Giappichelli, 2018, p. 470, che ritiene che la connessione tra i due beni emerga anche dalla disciplina a tutela della privacy.

[469] Così PICOTTI, FLOR, SALVADORI, *Reati contro l'inviolabilità del domicilio, la tutela della vita privata e dei segreti, la libertà e la personalità informatica*, *Relazione e proposta di articolato*, consultabile al sito istituzionale dell'Associazione dei professori di diritto penale, nella sez. documenti, quale risultato del gruppo di lavoro incaricato di avanzare proposte per la riforma dei delitti informatici contro la persona. In particolare, gli Autori individuano la cd. triade CIA quale nucleo fondamentale comune degli interessi giuridici meritevoli con riferimento alle fattispecie penali in materia di violazioni della riservatezza e sicurezza informatiche.

[470] In questi termini BRIGHI-CHIARA, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, in *federalismi.it* del 8 settembre 2012, p. 19.

[471] BRIGHI-CHIARA, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, *cit.*, p. 23, secondo cui "*l'esigenza di sicurezza, in ambienti complessi di interazione tra persone, software e servizi, rimanda dunque a una dimensione olistica di controllo del rischio che comporti la protezione in modo coordinato dei molti valori in gioco*".

già al fine di colmarne la frammentarietà, ma per offrire nuove occasioni sistematiche di verifica della coerenza ordinamentale"[472].

Pur condividendo la valenza critica di un tale approccio, certamente funzionale alla prospettiva penale, esso non è riferibile alla *cybersecurity* in cui la portata unificante va oltre la mera sommatoria di interessi eterogenei, operando in chiave unitaria di "contesto tecnocratico" e globale.

Da quanto sopra deriva non solo l'impossibilità di replicare, rispetto alla sicurezza informatica, concezioni onnicomprensive a carattere funzionale, ma anche il rifiuto di costruzioni ideologiche artificiali[473], dato che sono in gioco rapporti reali e concreti fra persone ed enti.

I risvolti in termini penalistici diretti della ricostruzione prospettata attengono, prima di tutto, alla formulazione delle disposizioni incriminatrici delle condotte con cui si manifestano fenomeni criminali che sfruttano l'interazione tra regola giuridica e tecnica, tipica delle attività illecite in ambito informatico o digitale; ed in secondo luogo all'imposizione sotto la minaccia anche della sanzione penale, "*di procedure (regole legislative, amministrative e organizzative), la predisposizione di meccanismi di controllo e la promozione di comportamenti individuali corretti per il controllo del rischio. Il rischio non rappresenta solo una condizione individuale, della persona singola che utilizza le ICT ma, in determinati contesti e scenari, diviene di interesse globale e riguarda questioni di sicurezza pubblica*"[474].

2. Considerazioni di stile.

I riflessi sostanziali delineati, proprio per la dimensione tecnica predominante, ricadono, in prospettiva *de iure condendo*, sulla formulazione delle relative fattispecie, quale necessità di tradurre in termini linguistici conformi l'intreccio tra regole giuridiche e regole tecniche.

In proposito non si tratta, come sostenuto da alcuni autori, d'individuare solo il "*punto di giusto equilibrio tra la preservazione dei principi di legalità, tassatività e determinatezza e la necessaria elasticità delle norme incriminatrici che, senza pregiudicare il requisito della prevedibilità e conoscibilità dei limiti entro i quali la condotta deve ritenersi lecita, possa abbracciare (e consentire di punire) comportamenti contra jus che*

[472] In questi termini PALAVERA, *Beni comuni e sistema penale*, in *disCrimen* dal 23.6.2021, p. 12 che concepisce un bene comune di tal fatta come "*argomento di selezione delle opzioni di tipizzazione (…) parametro rafforzato di verifica dell'efficacia attesa dalle politiche criminali*".

[473] Cfr. PICOTTI, *Sicurezza, informatica e diritto penale*, *cit.*, p. 232 che specifica come l'assenza di artificialità derivi, da un lato, dalla sua "*connotazione tecnica ben più precisa ed oggettiva, empiricamente "testabile", dato l'intreccio strutturale delle regole, anche giuridiche, con l'automazione*", dall'altro, dalla "*necessità condivisa nella società dell'informazione, per vedere garantita la certezza dei rapporto interpersonali, economici e sociali e giuridici, che in misura crescente si svolgono tramite le nuove tecnologie*".

[474] Testualmente BRIGHI-CHIARA, *op. ult. cit.*.

rappresentino naturali sviluppi di condotte devianti poste in essere con mezzi e metodi messi a disposizione della evoluzione tecnico-scientifica"[475].

Una lettura di questo tipo tradisce nella sostanza i rilievi assiologici sopra riconosciuti, confinando l'evoluzione tecnica in una logica di strumentalità, che non è declinabile rispetto a quella digitale.

Non appare per ragioni analoghe nemmeno condivisibile quella tendenza, manifestata da altra parte della dottrina[476], alla incriminazione dei fenomeni informatici in termini definitori tradizionali, mediante mero recepimento "ai fini penali" delle corrispondenti nozioni tecniche, che comporterebbe quell'immobilismo che deve essere, in ogni caso, evitato, perché incompatibile sia con la natura dinamica della rete, sia con quella evolutiva delle TIC[477].

Proprio perché *"l'informatica condiziona fin dall'origine, definendone i termini, il lavoro del giurista"* [478], come è stato autorevolmente messo in evidenza, bisogna ricorrere ad una "*semantica tecnica che possa riempire termini "tradizionali", comprensibili al giurista ed all'opinione pubblica, con contenuti adattabili al nuovo contesto tecnologico, attenendosi quanto più fedelmente possibile sia al testo redatto dal legislatore, sia ai significati correnti di un termine attribuiti dalla realtà o, meglio, dalla regola tecnologica*"[479].

In virtù di quanto sopra appare praticabile una "*rappresentazione tipologica*" di natura tecnica del fatto tipico, la quale, in virtù del sostrato tecnologicamente apprezzabile, potrebbe avere un grado di descrizione e comprensione paragonabile alla "*rappresentazione figurativa*"[480].

In questo modo sarebbe rispettata la legalità penale, intesa come *"preesistenza di un parametro di giudizio vincolante nel suo limite esterno, che consenta una duplice e complementare funzione: da un lato, la*

---

[475] Così FUMO, *"Res telematica". La problematica corporeità del file ed il reato di appropriazione indebita nota a sentenza appropriazione*, in *Rivista di diritto dei media*, 2/2020, p. 282.

[476] FUMO, *La condotta nei reati informatici*, *cit*., p. 777, secondo cui "*per un corretto inquadramento dei "termini della questione", bisognerebbe che fosse soddisfacentemente risolta la "questione dei termini"; ciò per dare concretezza ai confini delle condotte descritte con parole "prese a prestito" da altri universi semantici e per fornire certezze all'interprete*".

[477] FLOR, *Riservatezza informatica e sicurezza informatica quali nuovi beni giuridici penalmente protetti*, cit., p. 474, ritiene che "*A fenomeni "in movimento" dovrebbero corrispondere, da un lato, settori dell'ordinamento ad elevato coefficiente di adattamento e, dall'altro lato, un diritto giudiziale flessibile*".

[478] FINOCCHIARO, *Riflessioni su Diritto e Tecnica*, in *Dir. informatica*, 4-5/2012, p. 831.

[479] FLOR, *op. ult. cit.;* nella stessa direzione sostanziale DONINI, *La scienza penale integrale fra utopia e limiti garantistici,* in MOCCIA, CAVALIERE (a cura di), *Il modello integrato di scienza penale di fronte alle nuove questioni sociali*, Napoli, 2016, p. 43, per cui "*il Parlamento dovrà attrezzarsi per costruire prima, e il penalista per impiegare poi, le sue 'competenze', tenendo conto delle conoscenze dei settori tecnici di riferimento. In caso contrario sarà impossibile una disciplina razionale o adatta allo scopo*".

[480] Cfr. PAPA, *La tipicità iconografica della fattispecie e l'interpretazione del Giudice. La Tradizione illuministica e le sfide del presente*, in CONTE, LANDINI (a cura di), *Principi, regole, interpretazione. Contratti e obbligazioni, famiglie e successioni, Principi, regole, interpretazione. Contratti e obbligazioni, famiglie e successioni. Scritti in onore di Giovanni Furgiuele*, 2017, p. 339- 340. L'Autore si interroga sulla possibilità che, accanto alla fattispecie come rappresentazione del fatto vietato "*mediante una figurazione iconica*", ne sia possibile anche una "*definizione linguistica che, senza descrivere l'apparenza, la species del fatto tipico, ne elenchi semplicemente le proprietà rilevanti*", escludendo, in ogni caso, che "*l'indicazione del fatto vietato possa prescindere da un riferimento ad una forma paradigmatica del suo manifestarsi*".

limitazione dell'attività valutativa del giudice nell'identificazione dei fatti rilevanti; dall'altro lato, l'orientamento del comportamento del cittadino"[481].

Nella prospettiva delineata andrebbe, inoltre, valorizzato, in funzione integrativa degli elementi tipizzanti, il ricorso, promosso dalle fonti sovranazionali, a clausole di illiceità speciale- "senza diritto" o "indebitamente"- da riferire "*alla violazione di regole giuridiche extrapenali ovvero di condizioni desumibili dal contesto in cui opera l'agente relative non solo alla assenza di cause di giustificazione (quali il consenso dell'avente diritto, la legittima difesa, lo stato di necessità), ma anche alla competenza del soggetto ad agire, ovvero ad altri principi stabiliti dal diritto interno*"[482].

Queste clausole, al pari del requisito della fraudolenza, sono, ad avviso di chi scrive, idonee a colorare in termini personalistici/conflittuali quella compromissione che risponde alla descrizione normativa a valenza tecnologica, rinsaldando il connubio tra la norma tecnica e quella giuridica: la rilevanza penale sarebbe, così, veicolata dalla violazione delle competenze e prerogative spettanti al singolo, quale proiezione offensiva alla regolamentazione degli interessi personali mediati dall'informatica. Sotto questo profilo l'individuazione della tipicità passerebbe, cioè, attraverso l'ancoraggio della valutazione del giudice a parametri inerenti il contesto relazionale-fattuale di base[483].

In questo senso sembra valorizzabile anche la strutturazione delle fattispecie penali a dolo specifico, purché il ricorso a componenti intellettive e volitive non sia concepito come meramente compensativo di qualcosa che è materialmente mancante, ma valorizzato in funzione esplicativa di una condotta base che, per il suo oggetto, per la complessità dei rapporti sociali o per le sue forme di manifestazione dell'offesa, non è descrivibile in termini solo oggettivi[484].

---

[481] In questi termini con riferimento alla "*formalità*" della legalità penale PAONESSA, *Parola e linguaggio nel diritto penale: la garanzia della forma oltre il formalismo*, in *Studi Senesi*, vol. CXXIX, p. 308

[482] Testualmente *PICOTTI, Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale, cit.*, p. 197-198, che evidenzia come queste clausole siano, unitamente al carattere intenzionale, elemento comune di tutte le fattispecie considerate dalla Convenzione Cybercrime, ad eccezione di quelle in materia di diritto d'autore.

[483] DI MARTINO, *Tipicità di contesto. A proposito dei c.d. indici di sfruttamento nell'art. 603-bis c.p.*, in *Archivio penale*, 3/2018, p. 48 ss., con considerazioni a valenza generale, si esprime favorevolmente ad una formulazione della fattispecie che ne valorizzi il contesto fattuale costituente "*la ragion d'essere dell'intervento penale, prima ancora che l'ambito materiale d'applicazione della fattispecie tipica dal punto di vista strettamente normativo*" poiché delimitante "*la specifica rilevanza penale del fatto*".

[484] In questi termini PICOTTI, *Il dolo specifico. Un'indagine sugli "elementi finalistici" delle fattispecie penali*, *cit.*, p. 545-546, il quale a p. 583 specifica anche come non si tratta "*tanto di oggettivare arbitrariamente un dato in realtà soggettivo (nel senso naturalistico di "psichico"), bensì di riconoscere che è lo stesso legislatore a voler esprimere- attraverso il peculiare richiamo ad un elemento della fattispecie legale descritto in termini "finalistici"- un contenuto di sintesi oggettivo*".

Solo se inteso in questi termini, l'espressione attraverso il fine della proiezione conflittuale intersoggettiva che connota il fatto permette che il delitto possa essere "*l'immagine legislativa più possibile individuale del torto*"[485].

Se per questa via il reato informatico può recuperare una dimensione interpersonale "realistica" che assume normativamente la portata della regola tecnica, la combinazione tra la regola tecnica e quella giuridica stenta a trovare un equilibrio sul piano della territorialità, la quale è connotazione estranea al reato informatico per "*l'assenza di frontiere fisiche nel cyberspazio (....) sicché appare impossibile delimitare l'ambito di operatività delle norme statali*"[486].

3. Locus commissi delicti e Locus "informatico".

La difficoltà di applicare al cyberspace ed in generale ai reati informatici la categoria dogmatica del *locus commissi delicti*[487] non è questione nuova, né per la dottrina, né tantomeno per la giurisprudenza[488].

---

[485] GALLO, *Il dolo. Oggetto e accertamento*, *cit.*, p. 240.

[486] MAESTRI, *Lex informatica e diritto. Pratiche sociali, sovranità e fonti nel cyberspazio*, in *Ars interpretandi*, 1/2017, p. 16-19, sostiene che "*Facendo leva sull'ingannevole e fuorviante metafora del cyberspazio come luogo (cyberspace as place), i tribunali applicano alle e-mail e all'accesso ai siti web la dottrina dell'illecita turbativa del possesso di cose, da un lato ignorando che nessuno «entra» in un sito web e dall'altro veicolando l'idea, errata e ridicola al contempo, che Internet sia un luogo in cui viaggiare. In realtà, nessuno si trova nel cyberspazio. Internet è semplicemente un protocollo, ossia una parte di codice che consente agli utenti di trasmettere dati fra computer tramite i network comunicativi esistenti*".

[487] Sull'origine e funzione di questa categoria Cfr. SINISCALCO, voce *Locus commissi delicti*, in *Enc. dir.*, XXIV, 1974, p. 1051 ss.. L'autore esclude che si possa individuare un criterio a valenza generale che fissi il luogo di consumazione, essendo questo dipendente dall'istituto rispetto alla quale si pone in via preliminare la questione della collocazione spaziale del reato.

[488] Senza pretesa di completezza, tra i vari contributi si rinvia a RUGGIERO, *Momento consumativo del reato e conflitti di giurisdizione nel ciberspazio*, in *Giur. merito*, 2002, p. 254 ss.; MANICCIA, *Gli incerti "confini" del principio di territorialità*, in *Cass. pen.*, 11/2008, p. 3717 ss.; ALESIANI, *Il momento consumativo del delitto di frode informatica: indicazioni contraddittorie della Cassazione,* in *Cass. pen.*, 2/2001, p. 481 ss.; SEMINARA, *Locus commissi delicti, giurisdizione e competenza nel cyberspazio,* relazione al Convegno "*Presi nella rete – Analisi e contrasto della criminalità informatica*", Pavia, 23 novembre 2012, reperibile su *www.informaticagiuridica.unipv.it/convegni/2012/SEMINARA*; con specifico riferimento alle truffe on line vedi CIPOLLA, *Il profitto "ubiquo": in tema di truffa on line e competenza territoriale*, nota a Cass. pen., sez. I, 13.03.2015, n.25230, in *Cassazione Penale*, 3/2016, p. 956 ss.; MINNITI, *Il momento consumativo della truffa realizzata mediante pagamento con bonifico bancario*, nota a Cass. pen. , sez. fer., 30.08.2016, n.37400, in *Ilpenalista.it* del 10.11.2016; SCHILLACI, *Sulla competenza per territorio nel reato di truffa online compiuto mediante accredito su carta postepay*, nota a Cass. pen., sez. II, 06.06.2019, n.49195, in *Ilpenalista.it* del 29.05.2020; con riguardo al delitto di accesso abusivo vedi C. PECORELLA, *L'attesa pronuncia delle sezioni unite sull'acceso abusivo a un sistema informatico: un passo avanti non risolutivo*, in *Cass. pen.*, 2012, 3681 ss.; GROSSO, *Su un'interessante controversia interpretativa in tema di luogo del commesso reato e di giudice competente per territorio in materia di accesso abusivo in un sistema informatico*, in *Riv. it. dir. proc. pen.*, 2014, 1518 ss.; BELLACOSA, *Il luogo di consumazione del delitto di accesso abusivo a un sistema informatico o telematico: in attesa delle sezioni unite*, in www.dirittopenalecontemporaneo.it del 2.02.2015; DE MARTINO, *Le Sezioni Unite sul luogo di consumazione dell'accesso abusivo a sistema informatico,* in www.dirittopenalecontemporaneo.it del 11.05.2015.

Quanto sopra assume dei contorni particolarmente problematici se consideriamo le caratteristiche tecniche della tecnologia DLT[489], che possono essere così sintetizzate: "*la condivisione e la sincronizzazione dei dati digitali secondo un algoritmo di consenso, la distribuzione geografica di copie equivalenti in vari punti del mondo, e l'assenza di un amministratore centrale*"[490].

Sotto questo profilo, si ritiene che siano ormai maturi i tempi per la previsione di criteri appositi di attribuzione della giurisdizione per i reati informatici, funzionali alla regolamentazione anche della competenza per territorio[491].

Non si tratta di rifiutare in toto l'impostazione conseguente alla combinazione del criterio dell'ubiquità, quale base per l'affermazione della giurisdizione italiana, e del luogo di consumazione del reato, temperato dai criteri secondari e residuali di cui all'art. 9 c.p.p., ai fini della competenza[492].

Ferma l'operatività, laddove possibile, di questi criteri, si intende sostenere per tale via il riconoscimento del cyberspace quale "luogo" di pari dignità di quello fisico, per cui prevedere parametri di allocazione spaziale che prescindano dai fattori ambientali individuati secondo i canoni tradizionali.

Secondo quanto sostenuto da autorevole dottrina con riferimento ai reati transnazionali, di cui il cyberspace-dato "l'assenza" di confini- rappresenta uno stadio tecnico di grado ulteriore, si tratterebbe di elaborare "*schemi nuovi e non necessariamente ancorati ai confini territoriali ed in grado, in ultima istanza, di intercettare l'attuale mobilità dei reati*"[493].

Un'operazione di questo tipo è utile, se si considera anche la sfasatura spazio-temporale tra il momento realizzativo e quello percettivo/durativo dell'offesa[494], che può connotare i reati

[489] Si rinvia in proposito al paragrafo 1 cap. II.

[490] Così MOMOT, TESLENKO, TUMIETTO, *Blockchain e DLT per la pubblica utilità: gli esempi più promettenti e i problemi da risolvere*, in www.agendadigitale.eu del 28 gennaio 2019.

[491] Sul legame esistente tra i due istituti ed in particolar modo sulla definizione della competenza come misura della giurisdizione e sul suo riparto per materia e per territorio vedi MARVULLI, *Competenza ed incompetenza penale*, in *Enc. dir.,* V agg., Milano, 2001, p. 117 ss..

[492] FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative, cit.*, p. 145, ritiene che "*Il principio di territorialità, dunque, costituisce il criterio-base che presiede alla disciplina relativa alla validità della legge penale nello spazio. Principio per il vero temperato dal contemporaneo ricorso ad altri criteri, ravvisati nei principi di personalità, difesa e universalità*".

[493] In questi termini ORLANDO, *Mobilità dei reati nello spazio transfrontaliero e nuovi confini delle norme penali: verso una giurisdizione "a geometria variabile"?,* in MILITELLO, SPENA (a cura di), *Mobilità, sicurezza e nuove frontiere tecnologiche, cit.*, p. 81.

[494] FLOR, *I limiti del principio di territorialità nel cyberspace. Rilievi critici alla luce del recente orientamento delle Sezioni Unite,* in *Diritto penale e processo, 10/2015,* p. 1297, per cui ""*Smaterializzazione*", "*velocizzazione*", "*deterritorializzazione*", "*ubiquità*" e "*detemporalizzazione*" *coinvolgono le condotte concrete, che prescindono o si distanziano dalla fisicità dei comportamenti o dei fatti esteriori – ossia dall'azione o dall'omissione tradizionalmente intese – capaci di "incorporare" l'accadimento materiale*".

informatici in senso ampio ed in specie quelli cibernetici e che mette in crisi la stessa determinazione del loro momento consumativo[495].

Nella ricerca di questi criteri non si intende né introdurre una norma generale definitoria della consumazione[496], che rimane questione presupposta da risolvere in via preliminare[497], né tradire i vincoli costituzionali e convenzionali discendenti dal principio di legalità, di cui è parte integrante il principio stesso del giudice naturale precostituito per legge[498].

Una concezione sostanziale della legalità penale come "*mezzo che assicura la possibilità generale della valutazione anticipata delle conseguenze comportamentali*"[499] può ritenersi rispettata in presenza di regole generali che evochino "*piuttosto la dimensione assiologica degli interessi da proteggere*"[500] e si pongano in connessione sostanziale con i poli della carica lesiva del fatto di reato. Questi poli sono l'autore e la vittima del reato[501], quali titolari di quella conflittualità vietata, immanente e necessaria

---

[495] PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme, cit*., p. 91. L'Autore partendo dalla considerazione che "*è lo stesso "fatto" tipico che, nella parte in cui si realizza tramite i sistemi informatici, si può ritenere che si protragga ed eventualmente "riproduca", in forza delle funzioni automatizzate di memorizzazione, trasmissione, messa a disposizione, condivisione*", sostiene che si debba procedere all'"*adattamento alla realtà cibernetica della tradizionale distinzione dogmatica fra momento di "perfezione formale" del reato, che si ha quando ne sono realizzati tutti gli elementi costitutivi essenziali, seppur nel loro contenuto minimo, e momento di "esaurimento" o "consumazione sostanziale", che si ha solo quando esso ha per l'appunto "esaurito" definitivamente il proprio specifico contenuto di offesa, avendo raggiunto il massimo grado di lesione del ben giuridico protetto. Ebbene, il reato cibernetico non può dirsi "esaurito" nel periodo intermedio anche assai lungo che può intercorrere fra i due momenti, in cui "permane" e si approfondisce l'offesa*". Vedi nella stessa prospettiva B. PANATTONI, *I riflessi penali del perdurare nel tempo dei contenuti illeciti nel cyberspace*, in www.sistemapenale.it del 22 maggio 2020. Discorre, invece, con riferimento ai reati cibernetici di "*funzionalizzazione del concetto di consumazione*" BRASCHI, *La consumazione del reato. Fondamenti dogmatici ed esigenze di politica criminale*, Cedam, 2020, p. 13.

[496] Per BRASCHI, *La consumazione del reato. Fondamenti dogmatici ed esigenze di politica criminale*, *cit*., p. 340, una norma generale sulla consumazione non è auspicabile in sé perché "*sarebbe eccessivamente generica e comunque infondata dal punto di vista politico-criminale*".

[497] Cfr. PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme, cit*., p. 93 che per i reati informatici in senso ampio individua il *locus commissi delciti* sulla base della regola dogmatica del perfezionamento formale "*salvo che l'evento "cibernetico" assuma immediati caratteri di "ubiquità" e perciò, non essendo possibile determinarlo, sia necessariamente quello "dell'ultimo luogo in cui è avvenuta una parte dell'azione o dell'omissione" (art. 9, comma 1, c.p.p.), con risultati in concreto non diversi da quelli collegati al menzionato criterio dell'"inizio della consumazione" previsto per il reato permanente (art. 8, comma 3, c.p.p.)*".

[498] MARVULLI, *Competenza ed incompetenza penale*, *cit*., p. 221 per cui questa garanzia sarebbe rispettata in forza di un'individuazione precostituita *ante factum* dalla legge. La predetta garanzia, che va letta in combinato disposto con il divieto di giudici straordinari o speciali di cui all'art. 102 cost., ha in realtà un contenuto più ampio, richiedendo anche indipendenza e imparzialità dell'organo decidente, come emerge dalla codificazione del medesimo principio all'art. 6 della Carta Europea dei diritti dell'uomo.

[499] Così MICHELETTI, *Reato e territorio*, in *Criminalia*, 2009, p. 578, il quale concepisce la legalità penale come strumento per un legittimo esercizio del potere punitivo, "*il portato della necessaria politicità del diritto (…) non si vede come si possa contestare che il fisiologico ambito di efficacia della legge penale deve coincidere, in via di principio, con il territorio in cui è in grado di esprimersi quella determinata opzione formale. "Validità normativa e reato", "potestà punitiva e reato", non possono che essere endiadi inscindibili, tali per cui non è nemmeno pensabile il secondo termine della relazione senza la presenza del primo*".

[500] Testualmente ORLANDO, *Mobilità dei reati nello spazio transfrontaliero e nuovi confini delle norme penali: verso una giurisdizione "a geometria variabile"?,* cit., p. 88.

[501] FLOR, *I limiti del principio di territorialità nel cyberspace. Rilievi critici alla luce del recente orientamento delle Sezioni Unite, cit*., p. 1307, ritiene possibile, con riferimento al delitto di accesso abusivo, in via interpretativa evolutiva

ad ogni forma di manifestazione criminale, rispetto ai quali deve operare la forza intimidatrice del precetto penale.

A questa logica sembrano ispirarsi le disposizioni sovranazionali successive alla convenzione di Budapest, ancora ancorata alla territorialità della condotta di reato in termini tradizionali[502], ed in particolare, le disposizioni della esaminata direttiva UE/713/2019, oltre che della direttiva UE/2018/1673 sulla lotta al riciclaggio mediante il diritto penale.

La prima, ispirata alla necessità che il riparto di giurisdizione garantisca che "*i reati di cui alla presente direttiva siano perseguiti in modo efficace*"[503], impone che "*Ciascuno Stato membro adotta le misure necessarie a stabilire la propria giurisdizione per i reati di cui agli articoli da 3 a 8 ove si verifichi uno o più dei casi seguenti: a) il reato è commesso, anche solo in parte, sul suo territorio; b) l'autore del reato è un suo cittadino. 2. Ai fini del paragrafo 1, lettera a), si ritiene che un reato sia stato commesso in tutto o in parte sul territorio di uno Stato membro quando l'autore commette il reato mentre era fisicamente presente in quel territorio e, indipendentemente dal fatto che il sistema di informazione con cui è stato commesso il reato si trovasse o meno nel suo territorio. 3. Uno Stato membro informa la Commissione ove decida di stabilire la giurisdizione per un reato di cui agli articoli da 3 a 8 commesso al di fuori del suo territorio, anche qualora: a) l'autore del reato risieda abitualmente nel suo territorio; b) il reato sia commesso a vantaggio di una persona*

---

del principio di territorialità, individuare il *locus commissi delicti* "*tramite il legame con il suo titolare. Di conseguenza la competenza dovrebbe essere riconosciuta al giudice del luogo in cui la vittima possiede il proprio centro di interessi (domicilio, sede dell'azienda ecc., a seconda dello "spazio informatico" violato, ossia "privato", "aziendale" ecc.), in quanto riconducibile a quell'area virtuale di espressione della sua intera personalità umana. Questa soluzione ermeneutica "evolutiva", da un lato, non risulterebbe incompatibile con il principio di universalità, o di tendenziale universalità, accolto dal nostro codice penale, anche nel caso di accessi provenienti dall'estero. Almeno parte della condotta abusiva (l'azione o l'omissione), infatti, si proietta sul sistema (rectius sull'espressione di un'area di pertinenza esclusiva di un soggetto) situato (fisicamente o virtualmente) in Italia, con la conseguenza che il reato si può considerare comunque commesso nel "territorio" dello Stato italiano (ex comma 2, art. 6 c.p.).Dall'altro lato si adatta alla complessità tecnica di infrastrutture o architetture logiche che potrebbe determinare l'impossibilità di conoscere con esattezza l'ubicazione dell'"area informatica" e dei dati nel cloud".*

[502] In tal senso FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative, cit.*, p. 150. Per maggiore chiarezza espositiva si riporta di seguito il testo dell'art. 22 della Convenzione Cybercrime sulla competenza: "*1.Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per stabilire la propria competenza per tutti i reati previsti in conformità agli articoli da 2 a 11 della presente Convenzione, quando i reati siano commessi: a. nel proprio territorio; b. a bordo di una nave battente bandiera della Parte; c. a bordo di un aeromobile immatricolato presso quella Parte; d. da un proprio cittadino, se l'infrazione è penalmente punibile là dove è stata commessa o se l'infrazione non rientra nella competenza territoriale di alcuno Stato. 2. Ogni Parte può riservarsi il diritto di non applicare o di applicare solo in condizioni o casi specifici le regole di competenza definite ai paragrafi 1.b - 1.d del presente articolo o in una parte qualunque di essi. 3. Ogni Parte deve adottare le misure che dovessero essere necessarie per stabilire la propria competenza in ordine alle infrazioni di cui all'articolo 24, paragrafo 1 della presente Convenzione, nel caso in cui l'autore presunto dell'infrazione si trovi nel proprio territorio e 18 non è estradabile verso un'altra Parte solo in virtù della sua nazionalità, dopo una richiesta di estradizione. 4. La presente Convenzione non esclude alcuna competenza penale esercitata da una Parte in base al proprio diritto interno.5. Quando più di una Parte rivendica la propria competenza per una presunta infrazione prevista dalla presente Convenzione, le Parti coinvolte si consultano, laddove sia opportuno, al fine di stabilire la competenza più appropriata per esercitare l'azione penale*".

[503] In questi termini il considerando 20 della direttiva UE/2019/713.

giuridica che ha sede nel suo territorio; c) il reato sia stato commesso contro uno dei suoi cittadini o contro una persona che risiede abitualmente nel suo territorio"[504].

Criteri di giurisdizione di questo tipo, accompagnati da meccanismi comunicativi-risolutivi di possibili conflitti tra gli Stati, ricalcano quell'impostazione procedurale e sostanziale adottata da fonti precedenti, come la direttiva c.d. "pif" UE/2017/1371 del Parlamento europeo e del Consiglio, recante norme per la lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale[505], nonché la direttiva UE/2013/40, relativa agli attacchi contro i sistemi di informazione, che all'art. 12, comma 2, consente la fissazione della giurisdizione nello Stato membro in cui "*l'autore abbia commesso il reato mentre era fisicamente presente nel suo territorio, indipendentemente dal fatto che il reato sia stato o meno commesso contro un sistema di informazione nel suo territorio; b) il reato sia stato commesso contro un sistema informativo nel suo territorio, indipendentemente dal fatto che l'autore del reato fosse o meno fisicamente presente nel suo territorio al momento della commissione del reato*"[506].

Come evidenziato da dottrina autorevole[507], questi criteri consentono il radicamento della giurisdizione secondo una prospettiva sostanziale, di corrispondenza con la presenza fisica del titolare del centro d'interessi violato o ancora dell'autore di questa violazione.

In questi termini possono essere lette anche le disposizioni della direttiva UE/2018/1673 relativa alla lotta al riciclaggio, le quali seguendo una logica efficientista volutamente estensiva[508], replicano di fatto i medesimi criteri, individuando come risolutivi, nel caso di conflitto di giurisdizione, i seguenti fattori: "*a) il territorio dello Stato membro in cui è stato commesso il reato; b) la cittadinanza o la residenza dell'autore del reato; c) il paese d'origine della vittima o delle vittime; d) il territorio in cui è stato rinvenuto l'autore del reato*"[509].

---

[504] Così art. 12 della direttiva UE/2019/713.

[505] ORLANDO, *Mobilità dei reati nello spazio transfrontaliero e nuovi confini delle norme penali: verso una giurisdizione "a geometria variabile"?,* cit., p. 105.

[506] FLOR, *I limiti del principio di territorialità nel cyberspace. Rilievi critici alla luce del recente orientamento delle Sezioni Unite, cit.*, p. 1309, ritiene che una lettura sistematica di questa previsione unitamente all'art. 22 della Convenzione Cybercrime "*consentirebbe di attrarre la competenza e la giurisdizione sia nel caso in cui l'agente ed il sistema della vittima si trovino nel territorio dello Stato, sia quando solo il sistema attaccato si trovi nel territorio dello Stato, anche se l'attaccante si trova all'estero*".

[507] FLOR, *op. cit.*, p. 1308, ritiene che criteri di tal fatta consentano con riferimento al delitto di accesso abusivo di concentrare la regola sulla competenza sul legame "*fra titolare, "spazio informatico" e bene giuridico protetto*".

[508] Sulla base del Considerando 17 della direttiva UE/2018/1673 "*la mobilità degli autori dei reati e dei proventi derivanti dalle attività criminose, così come la complessità delle indagini transfrontaliere necessarie per contrastare il riciclaggio*" dovrebbero richiedere che "*tutti gli Stati membri dovrebbero stabilire la propria competenza giurisdizionale per consentire alle autorità competenti di indagare su tali attività e avviare azioni penali. Gli Stati membri dovrebbero pertanto garantire che la loro competenza giurisdizionale includa le situazioni in cui un reato è commesso per mezzo di tecnologie dell'informazione e della comunicazione dal loro territorio, indipendentemente dal fatto che tali tecnologie siano basate o meno sul loro territorio*".

[509] Così l'art. 10 della direttiva 1673/2018 di cui si riporta di seguito, per una migliore comprensione, il testo integrale: "*1. Ciascuno Stato membro adotta le misure necessarie per stabilire la propria competenza giurisdizionale per i reati di cui agli articoli 3 e 4 nei seguenti casi: a) il reato è commesso, anche solo parzialmente, nel suo territorio; b) l'autore del reato è un suo cittadino. 2. Uno Stato membro informa la Commissione in merito alla decisione di estendere*

Pur condividendo le frizioni che disposizioni di tal fatta innescano nel sistema delle condizioni di procedibilità delineato dall'art. 9 c.p.[510] e ferma la necessità di una revisione dei criteri di giurisdizione e competenza in chiave sovranazionale e coordinata da un punto di vista investigativo, la "territorializzazione" sulla base della presenza fisica dell'agente o del centro d'interessi pregiudicato[511], in questo modo riferibile anche alla persona offesa che abbia natura giuridica, si adatta alla dimensione aterritoriale dell'attuale contesto sociale ed economico, recuperando, però, una visione spaziale antropocentrica conforme alla forza soprattutto orientatrice del diritto penale[512].

4. Verso profili procedurali di responsabilità a garanzia della sicurezza informatica.

Una visione antropocentrica di questo tipo, che guarda alla rilevanza degli interessi in gioco, è compatibile anche con la tutela collettiva, in termini procedurali preventivi, della sicurezza in sé delle strutture informatiche che erogano i servizi economici e finanziari digitali.

La questione è destinata ad essere centrale nella definizione del regime giuridico dei servizi ed operatori FinTech, visto altresì che con la "Strategia per la finanza digitale"[513] la Commissione ha

---

la propria giurisdizione ai reati di cui agli articoli 3 e 4 commessi al di fuori del suo territorio quando: a) l'autore del reato risiede abitualmente nel suo territorio; b) il reato è commesso a vantaggio di una persona giuridica stabilita nel suo territorio. 3. Se un reato di cui agli articoli 3 e 4 rientra nella giurisdizione di più Stati membri, ciascuno dei quali sia legittimato a esercitare l'azione penale in relazione ai medesimi fatti, gli Stati membri in questione collaborano per stabilire quale di essi perseguirà l'autore del reato, al fine di accentrare l'azione penale in un unico Stato membro. Si deve tenere conto dei seguenti fattori: a) il territorio dello Stato membro in cui è stato commesso il reato; b) la cittadinanza o la residenza dell'autore del reato; c) il paese d'origine della vittima o delle vittime; e d) il territorio in cui è stato rinvenuto l'autore del reato. Se del caso, e conformemente all'articolo 12 della decisione quadro 2009/948/GAI, la questione è deferita a Eurojust".

[510] MAINIERI, *La Direttiva UE n. 1673/2018 sulla lotta al riciclaggio mediante il diritto penale: osservazioni sul recepimento*, nella sezione approfondimenti-antiriciclaggio di *www.dirittobancario.it* del 18.12.2020, evidenzia come a formulazione invariata dell'art. 9 c.p. il delitto di autoriciclaggio commesso interamente all'estero dal cittadino italiano sarebbe perseguibile nel nostro paese soltanto dietro richiesta del ministro della giustizia, essendo punito nel minimo con la reclusione di due anni. L'Autore mette in luce anche, come in forza dell'art. 4 d.lgs. 231/2001, la ricorrenza di questa richiesta condiziona la punibilità pure dell'ente.

[511] In questo senso, con riferimento alla presenza fisica del soggetto passivo titolare di un diritto al risarcimento, analogamente a quanto stabilito dal codice penale francese e nel nostro ordinamento in caso diffamazione, vedi CAMPLANI, *Locus commissi delicti, norme di collegamento e reati informatici a soggetto passivo indeterminato,* in *Archivio penale, 2/2020,* p. 32-33, secondo cui, a fronte dell'inapplicabilità di questa soluzione per i reati informatici a soggetto passivo indeterminato, per questi reati andrebbe preferito o il luogo in cui i dati informatici sono inseriti o quello in cui il soggetto attivo risiede o dimora; per l'Autore questa soluzione, da adottare in prospettiva unificatrice sovranazionale, "*si presenta come del tutto innovativa e per certi versi originale rispetto alla tradizione del diritto penale, ma potrebbe consentire di raggiungere obiettivi molto ambiziosi nel contrasto alla criminalità informatica*".

[512] Per tale si intende quella che viene definita da DE VERO, *Corso di diritto penale*, Giappichelli, Torino, 2020, p. 24-25, la dimensione positiva in senso stretto della prevenzione generale, di " *orientamento culturale verso l'acquisizione ed identificazione di qui valori che sono tutelati dalla norma penale*", che laddove "*orientata in chiave pedagogica riesce a conciliarsi armonicamente con- anzi finisce essa stessa per presupporre- quei principi di proporzionalità e di personalità della responsabilità penale destinati altrimenti a proporsi come limiti certo irrinunciabili, ma esterni e sostanzialmente confliggenti con la vocazione preventiva della pena*".

[513] Si rinvia in proposito alla nota 24.

presentato anche la Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo alla resilienza operativa digitale per il settore finanziario[514].

Nello specifico, con questa proposta si intende promuovere l'introduzione di un quadro generale per tutti gli aspetti della resilienza operativa digitale del settore finanziario, da affiancare al riesame in corso della direttiva n. 2016/1148, cd. NIS[515], con il quale di per sé si intende ampliare le categorie di destinatari delle prescrizioni, includendo i diversi settori rispetto ai quali la sicurezza informatica deve essere garantita[516].

Si tratta, per lo più, di oneri gestionali di prevenzione e monitoraggio, nonché di controllo, tempestiva rimozione e segnalazione alle autorità competenti degli "incidenti gravi" connessi alle TIC[517].

Questi oneri sembrano destinati ad incrementarsi laddove l'erogazione digitale del servizio si accompagni anche all'impiego di strumenti d'Intelligenza Artificiale, i quali aumentano le esigenze di tutela afferenti direttamente ai livelli di protezione della *cybersecurity*[518] e della *privacy*[519].

Proprio per la natura contestualmente vantaggiosa[520], ma anche imprevedibilmente pericolosa dei sistemi d'Intelligenza Artificiale, soprattutto "*pensanti*"[521], in prospettiva penale bisognerà valutare quali aree, rispetto a quelle costituite dalla programmazione, aggiornamento e manutenzione di

---

[514]Questa Proposta di regolamento, anche detta DORA-*Digital Resilience Operational Act* è consultabile al sito istituzionale della Commissione Europea.

[515] Senza alcuna pretesa di esaustività si rinvia in ordine alla portata e contenuti di questa direttiva, attuata in Italia con il d.lgs. 18 maggio 2018, n. 65, e agli ulteriori interventi nazionali che vi hanno fatto seguito D'AGOSTINO, *Cybersecurity, (auto)regolazione e governance del rischio. Quid de iure poenali?*, in *Luiss Dream Law Review*, n. 2/2017, p. 126 ss.; FLOR, *Cybersecurity ed il contrasto ai cyber-attacks a livello europeo: dalla cia-triad protection ai più recenti sviluppi,* in *Diritto di Internet,* 3/2019 p. 443 ss.; ROMOLOTTI, *Cybersecurity: un ponte tra GDPR e d.lgs. 231/2001 alla luce del d.lgs. 101/2018*, in *La responsabilità amministrativa della società e degli enti*, 2/2019, p. 71 ss..

[516] Sul punto diffusamente CICCIA ROMITO, *Verso la Direttiva NIS 2: la Cybersecurity al centro dei processi*, in *Quotidiano giuridico* del 4 maggio 2021, che rileva come "*nel disegno nostrano ed europeo, manca ancora l'attenzione alle micro e piccole, medie imprese: segno che la strada è ancora da definire, soprattutto alla luce dell'importanza rivestita dalla categoria nel tessuto economico europeo*".

[517] La proposta di regolamento definisce come tali un evento imprevisto, derivante o meno da attività dolose, che comprometta la sicurezza delle informazioni trattate, conservate o trasmesse, o che abbia effetti pregiudizievoli potenzialmente elevati sulla disponibilità, la riservatezza, la continuità o l'autenticità dei servizi finanziari forniti dall'entità finanziaria e specificatamente sulle sue funzioni critiche.

[518] DI CIOMMO, *La consulenza finanziaria automatizzata,* in CASSANO, DI CIOMMO, DE RITIS (a cura di), *Banche, Intermediari e Fintech, Nuovi strumenti digitali in ambito finanziario*, *cit*., p. 123.

[519] CONSOB, *La digitalizzazione della consulenza in materia di investimenti finanziari, cit*., p. 98-99.

[520] In questo senso MORERA, *Consulenza finanziaria e robo-advisor: profili cognitivi*, in FIMMANÒ, FALCONE (a cura di), *FinTech*, *cit*., p. 203 ss., che individua tra i vantaggi che derivano in particolare dall'utilizzo di *robo advisor* la maggiore democraticità ed economicità del servizio, nonché la sua capacità individuativa di prodotti differenti.

[521] PIERGALLINI, *Intelligenza Artificiale: da 'mezzo' ad 'autore' del reato?*, in *Riv. it. dir. proc. pen*., 4/2020, p. 1749 definisce così i sistemi di autoapprendimento connotati dalla "*prevedibilità dell'imprevedibilità" (autointegrabile dal 'demone')*".

questi sistemi[522], siano effettivamente suscettibili di una disciplina penale foriera di profili di responsabilità soprattutto omissivi, da inosservanza dello standard di sicurezza imposta.

Con specifico riferimento ai servizi economici e finanziari digitali, appare, inoltre, opportuno valutare anche il ruolo del cliente/*user* che consapevolmente- nella scelta del servizio o prestazione resa mediante questi strumenti- si esponga al rischio oltre la soglia tollerabile.

La Commissione europea intende, infatti, puntare sulla finanza digitale "*per il bene dei consumatori e delle imprese*", garantendo, da un lato, "*che il quadro normativo dell'UE in materia di servizi finanziari non imponga né impedisca l'utilizzo di determinate tecnologie*", dall'altro, volendo "*conferire un ruolo attivo ai consumatori e di proteggerli costantemente, affinché possano beneficiare di un accesso più ampio a prodotti e servizi innovativi in condizioni di sicurezza*"[523]. Sembra, quindi, che l'inclusione e "alfabetizzazione" finanziaria debbano condurre ad una rivalutazione del ruolo degli utenti, che è destinata ad avere ricadute anche in ambito penale, magari rivedendo quella "*retorica della difesa del risparmiatore*"[524], che ha caricato la truffa di una dimensione macroeconomica che non le compete[525].

In questa direzione depone, altresì, la proposta di Regolamento in materia di Intelligenza Artificiale[526], presentata dalla Commissione il 21 aprile 2021, che si pone come obiettivi da raggiungere: "*(a) harmonised rules for the placing on the market, the putting into service and the use of artificial intelligence systems ('AI systems') in the Union; (b) prohibitions of certain artificial intelligence practices; (c) specific requirements for high-risk AI systems and obligations for operators of such systems; (d) harmonised transparency rules for AI systems intended to interact with natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content;(e) rules on market monitoring and surveillance*"[527].

---

[522] LIACE, *Robo-advisor e finanza comportamentale*, in FIMMANÒ, FALCONE (a cura di), *FinTech*, *cit*., p. 202, discorre in proposito di responsabilità da algoritmo o da software e dell'aggiunta accanto alle asimmetrie informative di quelle tecnologiche.

[523] Si tratta della Comunicazione della Commissione Europea sulla strategia della finanza digitale, per cui si rinvia per i riferimenti del caso alla nota 24.

[524] In questi termini MAGRO, *Paternalismo penale e tutela dell'investitore dal rischio finanziario*, cit., p. 208, per cui la questione di fondo non è la tutela del risparmiatore in quanto vittima in sé, ma che "*la truffa, sebbene costituita come condotta che si avvantaggia di una informazione asimmetrica, ben poco può fare di fronte a sistemi finanziari complessi, in cui non sempre tutto ciò che è rilevante deve essere comunicato obbligatoriamente, o in cui l'informazione tecnica non basta a ristabilire una parità in termini di potere contrattuale e di effettiva partecipazione alla formazione della volontà negoziale*".

[525] Sul punto si rinvia alle note 54 e 55.

[526] Si tratta della proposta COM(2021) 206 final a cui si collega il piano coordinato sull'Intelligenza Artificiale 2021, per la cui consultazione si rinvia al sito istituzionale della Commissione Europea. Per un primo commento sulla proposta si rinvia alla newsletter di aprile 2021 dell'Osservatorio Cybercrime dell'Università di Verona consultabile al sito https://sites.les.univr.it/cybercrime/. In argomento cfr. LA VATTIATA, *Brevi note "a caldo" sulla recente Proposta di Regolamento UE in tema di intelligenza artificiale,* in *www.dirittopenaleuomo.org* del 30.06.21.

[527] Così testualmente l'art. 1 della Proposta di cui si riporta di seguito il relativo testo in italiano: *"Il presente regolamento stabilisce: a)regole armonizzate per l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di intelligenza artificiale ("sistemi di IA") nell'Unione; a)il divieto di determinate pratiche di intelligenza artificiale;*

L'approccio prescelto è basato sul livello di rischio[528], conformemente al quale si intende creare un sistema di *governance* dell'Intelligenza Artificiale.

Rispetto a tale prospettiva è da comprendere se e in che termini potrà contribuire il diritto penale: se, cioè, la sicurezza, che si intende garantire mediante l'imposizione di obblighi variamente modulabili in funzione di tutela dei diritti dei singoli, passi anche attraverso la minaccia della sanzione punitiva massima, quale emerge dalle scelte d'incriminazione nazionale operate con il Perimetro di Sicurezza Cibernetico[529], individuando persone, enti o addirittura robot che ne debbano rispondere.

b)requisiti specifici per i sistemi di IA ad alto rischio e obblighi per gli operatori di tali sistemi; c)regole di trasparenza armonizzate per i sistemi di IA destinati a interagire con le persone fisiche, i sistemi di riconoscimento delle emozioni, i sistemi di categorizzazione biometrica e i sistemi di IA utilizzati per generare o manipolare immagini o contenuti audio o video)regole in materia di monitoraggio e vigilanza del mercato". Al considerando 5 è espressamente stabilito che "*Si rende pertanto necessario un quadro giuridico dell'Unione che istituisca regole armonizzate in materia di intelligenza artificiale per promuovere lo sviluppo, l'uso e l'adozione dell'intelligenza artificiale nel mercato interno, garantendo nel contempo un elevato livello di protezione degli interessi pubblici, quali la salute e la sicurezza e la protezione dei diritti fondamentali, come riconosciuti e tutelati dal diritto dell'Unione*".

[528] PIERGALLINI, *Intelligenza Artificiale: da 'mezzo' ad 'autore' del reato?*, *cit*., p. 1748, considera l'individuazione di questo livello come una scelta politica "*di taglio proattivo e non già reattivo, che non si orienta, cioè, in un'ottica consequenziale, concernente l'individuazione dei centri di responsabilità, ma che, prima ancora, prova a decidere come governare, preventivamente, questi rischi, interrogandosi sul livello di tollerabilità sociale*"

[529] Con specifico riferimento agli obblighi e connessi reati introdotti con il d.l. 105/2019, convertito con la legge 133/2019 vedi ROMOLOTTI, *Il decreto Cybersecurity e le nuove ipotesi rilevanti di reato ex d.lgs. 231/2001,* in *La responsabilità amministrativa della società e degli enti*, 2/20, p. 121 ss.; PICOTTI, VADALÀ, *Sicurezza cibernetica: una nuova fattispecie delittuosa a più condotte con estensione della responsabilità degli enti*, in www.sistemapenale.it, 5 dicembre 2019.

Indice bibliografico generale

ACCINNI, *Profili di rilevanza penale delle "criptovalute" (nella riforma della disciplina antiriciclaggio del 2017)*, in *Archivio penale* n. 1/2018, p. 1 ss.;

AIMI, *In tema di uso e appropriazione nell'ambito dei delitti di peculato,* in *Riv. it. dir. proc. pen.*, 2013, p. 2063 ss.;

ALCINI, *Mondi paralleli, "bitcoin" e reati virtuali*, in *La Giustizia penale*, 7/2018, p. 438 ss.

ALESIANI, *Il momento consumativo del delitto di frode informatica: indicazioni contraddittorie della Cassazione,* in *Cass. pen.*, 2/2001, p. 481 ss.;

AMATO, *Solo nei casi di "provenienza delittuosa" l'acquisto di carte di credito è ricettazione - La punibilità dell'illecito utilizzo esclude il ricorso con il reato di truffa*, in *Guida al diritto*, 29/2001, p. 58 ss.;

AMOROSO, *La sorte dei furti di generi di prima necessità all'interno dei supermercati all'indomani della pronuncia delle Sezioni Unite n. 52117/2014 e dell'introduzione dell'art. 131-bis nel codice penale*, nota a Cass. pen., S.U., 17.07.2014, n.52117, in *Cass. pen.*, 6/2015, p. 2168 ss.;

ANGIONI, *Contenuto e funzioni del concetto di bene giuridico*, Giuffrè, Milano, 1983;

ANSELMI, *Onion routing, cripto-valute e crimine organizzato*, *Quaderni del Centro Ricerca Sicurezza e Terrorismo*, Pacini Giuridica, 2019;

ANTOLISEI, *Manuale di diritto penale. Parte speciale*, vol. I, 16 ed., 2016;

AUGELLO-PESA, *La proprietà del trustee e il reato di appropriazione indebita*, in *Trusts e attività fiduciarie,* n. 4/2015, p. 335 ss.;

AZZALI, *Diritto penale dell'offesa e riciclaggio*, in *Riv. It. dir. Proc. Pen.*, 1993, p. 419 ss.;

BARILE, *Appropriazione indebita di file informatici: tra interpretazione estensiva e divieto di analogia. Il diritto penale è "cosa mobile"*, in *Sistema penale*, 3/21, p. 139 ss.;

BARTOLI, *La distinzione tra appropriazione e distrazione e le attuali esigenze di tutela patrimoniale*, in *Dir. pen. proc.*, n. 9/2001, p. 1137 ss.;

BARTOLI, *La frode informatica tra "modellistica", diritto vigente, diritto vivente e prospettive di riforma,* in *Dir. inf.*, 3/2011, p. 383 ss.;

BELLACOSA, *Il luogo di consumazione del delitto di accesso abusivo a un sistema informatico o telematico: in attesa delle sezioni unite*, in www.dirittopenalecontemporaneo.it del 2.02.2015;

BELTRANI, *Reati informatici e d.lgs. 231/2001 alla luce della legge di attuazione della Convenzione di Budapest*, in *La Responsabilità amministrativa delle società e degli enti*, 4/2008, p. 21 ss.;

BENEVENTO, *La truffa sussiste indipendentemente dalla prova dell'indisponibilità del bene oggetto di vendita online*, nota a Cass. pen., sez. II, n. 51551/2019, in *Diritto di internet*, 2/2020, p. 321 ss.;

BERGHELLA, BLAIOTTA, *Diritto penale dell'informatica e beni giuridici*, in *Cass. pen.*, n. 9/1995, p. 2329 ss.;

BERTOLINO, *Nuovi orizzonti dei delitti contro il patrimonio nella circonvenzione di incapace e nell'usura*, Giappichelli, Torino, 2010;

BIXIO, *Le valute virtuali nella V Direttiva antiriciclaggio*, in *Corriere tributario*, n. 25/2018, p. 1987 ss.;

BOCCHINI, *Lo sviluppo della moneta virtuale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in *Diritto dell'Informazione e dell'Informatica*, 1/2017, p. 27 ss.;

BONAIUTI, *Schemi di pagamento e valute virtuali*, in *Moneta e Credito*, vol. 72, 288/2019, p. 389 ss.;

BONCOMPAGNI, *Crimini informatici e criptovalute*, in CAPACCIOLI (a cura di), *Criptoattività, criptovalute e bitcoin*, Giuffrè, 2021, p. 302 SS.;

BRASCHI, *La consumazione del reato. Fondamenti dogmatici ed esigenze di politica criminale*, Cedam, 2020;

BRICOLA, *voce Teoria generale del reato*, in *Noviss. Dig. It.*, XIX, 1973, p. 7 ss;

BRIGHI, *La vulnerabilità nel cyberspazio*, in *Ars interpretandi*, 1/2017, p. 81 ss.;

BRIGHI, *Cybersecurity. Dimensione pubblica e privata della sicurezza dei dati*, in CASADEI, PIETROPAOLI (a cura di), *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Cedam, 2021, p. 135 ss.;

BRIGHI-CHIARA, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, in *federalismi.it* del 8 settembre 2012;

BRUNELLI, *Dal reato continuato alla continuazione di reati: ultima tappa e brevi riflessioni sull'istituto*, in *Cass. pen.*, 7-8/2009, 2749 ss.;

CAJANI, *La tutela penale dell'identità digitale alla luce delle novità introdotte dal d.l. 14 agosto 2013 n. 93 (convertito con modificazioni dalla l. 15 ottobre 2013, n. 119)*, in *Cass. pen.*, 3/2014, p. 1094 ss.;

CAJANI, COSTABILE, MAZZARACO, *Phishing e furto d'identità digitale. Indagini informatiche e sicurezza bancaria,* Giuffrè, Milano, 2008;

CAJANI, *Le truffe on line*, in PARODI (a cura di), *Diritto penale dell'impresa*, Giuffrè, 2017, p. 573 ss.;

CAJANI, *La frode informatica*, in PARODI (a cura di), *Diritto penale dell'impresa*, Giuffrè, 2017, p. 557 ss.;

CAMPLANI, *Locus commissi delicti, norme di collegamento e reati informatici a soggetto passivo indeterminato,* in *Archivio penale, 2/2020,* p. 1 ss.;

CAPACCIOLI, *Aspetti operativi e ricadute giuridiche delle cripto-attività,* in *Diritto di Internet*, n. 3/2019, p. 591 ss.;

CAPACCIOLI, *Riflessioni sulla tassazione delle criptovalute: wallet quale deposito?*, in *L'Accertamento*, 6/2020, p. 62 SS.;

CAPONERA, GOLA, *Aspetti economici e regolamentari delle «cripto-attività»,* in *Questioni di Economia e Finanza (Occasional Papers)* di Banca d'Italia, n. 484, Marzo 2019.

CAPPITELLI, *I confini della nozione di bene mobile nei delitti contro il patrimonio*, in *Cassazione penale*, 3/21, p. 924 ss.;

CAPUTO, *Dalla disintegrazione del reato continuato alla continuazione di reati. Osservazioni in ordine al calcolo dell'aumento di pena*, in *Cass. pen.*, 3/2016, p. 1052 ss.;

CARMONA, *Tutela penale del patrimonio individuale e collettivo*, Mulino, 1996;

CARNELUTTI, *La tutela penale della ricchezza*, in *Riv. it. dir. pen.*, 1931, p. 7 ss.;

CASALE, *Prima "legge" della sicurezza informatica: "un computer sicuro è un computer spento"*, in *Archivio penale*, 2/2021, p. 5 ss.;

CASELLATO, DI MAIO, MUSCATELLA, *Il nodo gordiano dello "sviamento di potere" nell'accesso abusivo ad un sistema informatico, tra suggestioni dogmatiche e riflessioni giurisprudenziali*, in *Cass. pen.*, 7/2019, p. 2771 ss.;

CASTAGNO, STIGLIANO, *L'accesso abusivo a sistema informatico nell'era delle tecnologie dell'informazione e della comunicazione*, in *Diritto di internet*, 4/2019, p. 783 ss.;

CAUTERUCCIO, *I nuovi reati contro la fede pubblica: il falso in documento informatico pubblico o privato*, in *Rivista penale*, 10/2007, p. 965 ss.;

CATAUDELLA, *voce Fattispecie*, in *Enc. dir.*, vol. XVI, 1967, p. 926 ss.;

CHIARI, *Uso indebito di carte di credito e truffa: concorso di reati o assorbimento?*, in *Quotidiano Giuridico* del 4 agosto 2017;

CHIAROTTI, voce *Appartenenza*, in *Enc. dir.*, vol. II, 1958, p. 704 ss.;

CIAN, *La criptovaluta-alle radici dell'idea giuridica di denaro attraverso la tecnologia: spunti preliminari*, in *Banca Borsa Titoli di Credito*, 3/2019, p. 342 ss.;

CICCIA ROMITO, *Verso la Direttiva NIS 2: la Cybersecurity al centro dei processi*, in *Quotidiano giuridico* del 4 maggio 2021;

CINCOTTA, *Della falsità in monete, in carte di pubblico credito e in valori di bollo (artt. 453-466)*, in RAMACCI (a cura di), *I delitti contro la fede pubblica - Trattato di diritto penale*, Giuffrè, 2013, p. 103 ss.;

CIPOLLA, *E-commerce e truffa*, in *Giur. merito*, 12/2013, p. 2624 ss;

CIPOLLA, *Il profitto "ubiquo": in tema di truffa on line e competenza territoriale*, nota a Cass. pen., sez. I, 13.03.2015, n.25230, in *Cass. pen.*, 3/2016, p. 956 ss.;

CIPOLLA, *L'appropriazione indebita informatica nel contesto della dematerializzazione del concetto di cosa nei reati contro il patrimonio*, in *La Giustizia Penale*, 11/2020, p. 605 ss.;

CISLAGHI, *Ancora sul momento consumativo del delitto di furto*, in www.sistemapenale.it del 17 luglio 2015;

CISTERNA-LARUSSA, *I delitti di falso*, Cedam, 2010.

CLINCA, *L'incriminazione dell'autoriciclaggio tra tutela dell'ordine economico e garanzie fondamentali*, in www.lalegislazionepenale.eu, sez. approfondimenti del 3.5.2016;

COCCO, *Il falso bene giuridico della fede pubblica*, in *Riv. it. dir. proc. pen.*, 1/2010, p. 68 ss.;

COCCO, *Reato istantaneo, di durata e a più fattispecie. Questioni controverse di unità e pluralità*, in *Responsabilità civile e previdenza*, 2/2017, p. 374 ss.;

CONSO, FERRETTI, AMENDOLA, *Antiriciclaggio e valute virtuali*, in *Rivista della Guardia di Finanza*, 3/2020, p. 795 ss.;

CONIGLIARO, *La nuova tutela penale europea dei sistemi di informazione. Una prima lettura della direttiva 2013/40/UE del Parlamento Europeo e del Consiglio*, in www.penalecontemporaneo.it, del 30 ottobre 2013;

CORBETTA, *Furto di files*, in *Dir. pen. proc.*, 2/2011, p. 160 ss.;

CORBETTA, *Ladro che occulti la refurtiva: furto tentato o consumato?*, in *Dir. pen. proc.*, 5/2018, p. 626 ss.;

CORSARO, *Il recepimento della Direttiva PIF e le novità in materia di reati contro la pubblica amministrazione e reati tributari. L'ulteriore ampliamento dei reati presupposto per la responsabilità degli enti*, in www.giurisprudenzapenale.com del 20 luglio 2020;

COSSEDDU, *Riciclaggio: complessità di un "percorso" normativo*, in *Cass. Pen.*, 2010, p. 3641 ss;

CRESCIOLI, *La tutela penale dell'identità digitale*, in *Diritto Penale contemporaneo Rivista trimestrale*, 5/2018, p 265 ss.;

CRESPI, *Rassegna di diritto societario (1999-2000). Disposizioni penali in materia di società e consorzi*, in *Riv. delle so*cietà, 2-3/2002, p. 630 ss.;

CUCURACHI, *Lo sviluppo del FinTech a supporto della consulenza finanziaria agli investitori*, in BOSCIA, SCHIENA, STEFANELLI (a cura di), *Digital Banking e Fin tech. L'intermediazione finanziaria tra cambiamenti tecnologici e sfide di mercato,* Bancaria editrice, 2020, p. 225 ss.;

CUNIBERTI, *Tecnologie digitali e libertà politiche*, in *Diritto dell'Informazione e dell'Informatica, 2/2015, p*

L. D'AGOSTINO, *Cybersecurity, (auto)regolazione e governance del rischio. Quid de iure poenali?*, in *Luiss Dream Law Review*, 2/2017, p. 126 ss.;

L. D'AGOSTINO, *Operazioni di emissione, cambio e trasferimento di criptovaluta: considerazioni sui profili di esercizio (abusivo) di attività finanziaria a seguito dell'emanazione del D. Lgs. 90/2017*, in *Rivista di diritto Bancario*, 1/2018, p. 1 ss.;

L. D'AGOSTINO, *Offerte di criptoattività e abusivismo finanziario. I margini di rilevanza penale dell'esercizio non autorizzato di servizi di investimento*, nota a Cass. pen. Sez. II, 25.09.2020, n. 26807, in *Diritto di Internet,* 1/2021, p. 147 ss.;

D'AGOSTINO, *La tutela penale dei mezzi di pagamento della terza generazione*, in D'AMATO (a cura di), *Trattato di diritto penale dell'impresa*, Cedam, 1993, p. 470 ss.;

D'ANELLO, *Riciclaggio: dalla tutela penale del patrimonio individuale a quella dell'economia,* in *Archivio penale on line*, 2/2012, p. 1 ss.;

DAVOLA, *Distributed ledger technology, blockchain e mercati finanziari*, in CASSANO, DI CIOMMO, DE RITIS (a cura di), *Banche, Intermediari e Fintech, Nuovi strumenti digitali in ambito finanziario*, Giuffrè, 2021, p. 61 ss.;

DELL'ANNO, *Il delitto di riciclaggio: contrasto tra la previsione normativa e le applicazioni giurisprudenziali*, in *Cass. Pen.*, 11/2003, p. 3435 ss.;

DE AMICIS, *Contrasti giurisprudenziali in tema di "ricettazione" di carte di credito*, in *Cass. pen.*, 9/2000, p. 241 ss..

DELL'OSSO, *Riciclaggio di proventi illeciti e sistema penale*, Giappichelli, Torino, 2017.

DE MARISCO, *voce Falsità in atti*, in *Enc. Dir.*, vol. XVI, Milano, 1967, p. 560 ss.;

DE MARTINO, *Le Sezioni Unite sul luogo di consumazione dell'accesso abusivo a sistema informatico,* in *www.dirittopenalecontemporaneo.it* del 11.05.2015;

DE ROSA, *Il punto sull'analogia nel diritto penale: portata operativa del divieto e ruolo nell'attuale conflitto tra i poteri dello Stato*, in La *Giustizia penale*, 4/2012, p. 180 ss.;

DE VERO, *Corso di diritto penale*, Giappichelli, Torino, 2020;

DI CIOMMO, *La conclusione e l'esecuzione automatizzata dei contratti (smart contract),* in CASSANO, DI CIOMMO, DE RITIS (a cura di), *Banche, Intermediari e Fintech, Nuovi strumenti digitali in ambito finanziari,* Giuffrè, 2021, p. 79 ss.;

DI CIOMMO, *La consulenza finanziaria automatizzata,* in CASSANO, DI CIOMMO, DE RITIS (a cura di), *Banche, Intermediari e Fintech, Nuovi strumenti digitali in ambito finanziario*, Giuffrè, 2021, p. 117 ss.;

DI GIOVINE, *L'interpretazione nel diritto penale tra creatività e vincolo alla legge*, Milano, 2006;

DI GIOVINE, *L'attuale, il frainteso e il superato dell'ermeneutica penale nel contesto italiano*, in *Ars Interpretandi*, 2-2020, p. 67 ss.;

DI LERNIA, *Crowdfunding @ICOs: esigenze di prevenzione del rischio di commissione di reati nell'era della digital economy*, in *Diritto Penale Contemporaneo Rivista trimestrale*, 2/2019, p. 101 ss.;

A. DI MARTINO, *Tipicità di contesto. A proposito dei c.d. indici di sfruttamento nell'art. 603-bis c.p.*, in *Archivio penale*, 3/2018, p. 48 ss.;

DI MARTINO, *Soluzione e prospettive sulla "natura giuridica" delle valute virtuali*, in CASSANO, DI CIOMMO, DE RITIS (a cura di), *Banche, Intermediari e Fintech, Nuovi strumenti digitali in ambito finanziario*, Giuffrè, 2021, p. 279 ss.;

DI PAOLO, *Cyber crime. Il Phishing: prospettive di un delitto*, in *Archivio penale, 2/2017, p. 1 ss.;*

DI PORTO, STARITA, *La strategia europea sulla digitalizzazione e il posizionamenti dell'Italia*, in BOSCIA, SCHIENA, STEFANELLI (a cura di), *Digital Banking e Fin tech. L'intermediazione finanziaria tra cambiamenti tecnologici e sfide di mercato*, Bancaria editrice, 2020, p. 23 ss.;

DI VIZIO, *Lo statuto penale delle valute virtuali,* in *www.discrimen.it*, del 19 giugno 2019;

DI VIZIO, *Gli obblighi antiriciclaggio per operatori in valute virtuali*, Relazione al Seminario "*Monitoraggio del flussi finanziari e delle attività commerciali al fine di garantire la sicurezza europea-Conference on Security and Money Flows in the European Union*", organizzato dall'Unità di informazione Finanziaria per l'Italia, dalla Fondazione Bruno Kessler, BeSEC Boosting European Security Law and Policy e da Erasmus Programme of the European Union, Roma, 24—25 ottobre 2019, consultabile in *www.discrimen.it* del 2 dicembre 2019;

DONINI, *Abolitio criminis e nuovo falso in bilancio struttura e offensività delle false comunicazioni sociali (artt. 2621 e 2622 c.c.) dopo il d.lg. 11 aprile 2002, n. 61*, in *Cass. pen.*, 4/2002, p. 1240 ss.

DONINI, *Un nuovo medioevo penale? Vecchio e nuovo nell'espansione del diritto penale economico*, in *Cass. pen.*, 6/2003, p. 1808 SS.;

DONINI, *Il principio di offensività. Dalla penalistica italiana ai programmi europei*, in *Diritto penale contemporaneo*, 4/2013, p. 7 ss.;

DONINI, *Il diritto giurisprudenziale penale. Collisioni vere e apparenti con la legalità e sanzioni dell'illecito interpretativo*, in *Diritto penale contemporaneo Rivista trimestrale*, 3/2016, p. 1 ss.;

DONINI, *La scienza penale integrale fra utopia e limiti garantistici,* in MOCCIA, CAVALIERE (a cura di), *Il modello integrato di scienza penale di fronte alle nuove questioni sociali*, Napoli, 2016, p. 7 ss.;

DONINI, *Fattispecie o case law? La "prevedibilità del diritto" e i limiti alla dissoluzione della legge penale nella giurisprudenza*, in *Questione giustizia*, 4/2018, p. 79 ss.;

DURIGATO, *Rilievo sul reato plurioffensivo*, Cedam, Padova, 1972;

FALCINELLI, *Memento sulla tipicità penale dell'atto di disposizione del patrimonio*, in *Archivio penale*, 2/2012, p. 1 ss.;

FALCINELLI, *L'atto dispositivo nei delitti contro il patrimonio. Sezioni e intersezioni del sistema penale,* Giappichelli, Torino, 2013;

FALCINELLI, *Tempi moderni e cultura digitale: il valore patrimoniale dell'identità umana "on line"*, in *Ind. pen.*, 3/2015, p. 297 SS.;

FALCINELLI, *L'abuso del diritto in cerca di direzione penale Spunti dall'esegesi delle Sezioni unite sul delitto di mantenimento abusivo in sistema informatico*, in *Archivio penale*, 3/2017, p. 1 ss.;

FALDUTI, *Frode informatica e utilizzo indebito di carte di credito: variabili interpretative*, in *Giurisprudenza penale web*, 12/2017, p. 1 ss.;

FANELLI, *La truffa*, Giuffrè, Milano, 1998;

FARINELLA, *La Cassazione sulla configurabilità del reato di appropriazione indebita di files,* in *Indice penale*, 3/2020, p. 714 ss.;

FAVALORO, *Decreto Semplificazioni 2019: blockchain e smart contract diventano legge*, in *Quotidiano Giuridico* del 6 febbraio 2019;

FAZIO, *Cangiante profilo offensivo dei delitti di riciclaggio*, in *www.lalegislazionepenale.eu*, sez. approfondimento del 4.9.2020;

FERRARI, *Sui rapporti fra l'indebita percezione di erogazioni a danno dello Stato e la truffa aggravata per il conseguimento di erogazioni pubbliche*, in *Giur. It.*, 2004, p. 3 ss.;

FERRARI, *La nozione di possesso non cambia pelle nel passaggio dal campo civile al penale*, nota a Cass. pen., Sez. Un., 27.10.2004, n.1327, in *Diritto e Giustizia*, 5/2005, p. 38 ss.;

FERRARO, *Fintech. La digitalizzazione della finanza tra Criptovalute e Blockchain*, in *IPE Working Paper*, 18/2019, p. 3 ss.;

FIMMANÒ, FALCONE, *"FinTech": scenari, soggetti, temi*, in FIMMANÒ, FALCONE (a cura di), *FinTech*, Edizioni scientifiche Italiane, 2019, p. 1 ss..

FIORELLA, *voce Reato in generale*, in *Enc. Dir.*, XXXVIII, Milano, 1987, p. 770 ss;

FIORELLA, *L'economia pubblica e privata quale oggetto dell'offesa e parametro del campo di materia*, in *Riv. trim. dir. pen. econ.*, 3-4/2017, p. 455 ss.;

FIORELLA, *Lo sviluppo in Italia, nel '900, delle fondamentali categorie del diritto penale alla luce delle influenze della dottrina tedesca*, in *Rivista it. per le scienze giuridiche*, 6/2015, p. 173 ss..

FLICK, *La repressione del riciclaggio ed il controllo della intermediazione finanziaria. Problemi attuali e prospettive*, in *Riv. it. dir. Proc. Pen.*, 1990, p. 1265 ss;

FLOR, *Phishing e profili penali dell'attività illecita di "intermediazione" del cd. Financial manager*, in *Dir. pen. proc.*, 1-2012, p. 55 ss.;

FLOR, *Verso una rivalutazione dell'art. 615 ter c.p.?*, in *Diritto Penale contemporaneo Rivista trimestrale*, n. 2/2012, p. 126 ss.;

FLOR, *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di internet*, in *www.penalecontemporaneo.it* del 20.12.2012;

FLOR, *I limiti del principio di territorialità nel cyberspace. Rilievi critici alla luce del recente orientamento delle Sezioni Unite,* in *Dir. pen. proc.,* 10/2015, p. 1296 ss.;

FLOR, *Riservatezza informatica e sicurezza informatica quali nuovi beni giuridici penalmente protetti*, in MILITELLO, SPENA (a cura di), *Mobilità, sicurezza e nuove frontiere tecnologiche*, Giappichelli, 2018, p. 463 ss.;

FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime*, collana *Diritto e procedura penale dell'informatica*, utet, Torino, 2019, p. 145 ss.;

FLOR, *Cyber-criminality: le fonti internazionali ed europee*, in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime*, collana *Diritto e procedura penale dell'informatica*, utet, Torino, 2019, 98 e ss.;

FLOR, *Cybersecurity ed il contrasto ai cyber-attacks a livello europeo: dalla CIA-Triad Protection ai più recenti sviluppi*, in *Diritto di Internet*, n. 3/2019, p. 443 ss.;

FLOR, *Financial cybercrime & Cryptocurrencies: le prospettive applicative del diritto penale vigente*, in GUARDIA DI FINANZA (a cura di), *Atti della Giornata di studi "Le criptovalute: funzionamento, regolamentazione, profili applicativi e principali riflessi per la polizia economico finanziaria"*, Verona, 28 maggio 2019, p. 60 ss.;

FLOR, *Il diritto penale alla prova dell'hands-on dell'ethical hacking,* nota a Tribunale di Catania, Gip Rizza, decreto di archiviazione 15 luglio 2019, in *Diritto di internet*, n. 1/2020, p. 165 ss.;

FIANDACA, *Il diritto penale tra legge e giudice*, Cedam, 2002;

FIANDACA-MUSCO, *Diritto penale. Parte speciale*, vol. II, 7 ed., 2015, ;

FINOCCHIARO, *Riflessioni su Diritto e Tecnica*, in *Dir. informatica*, 4-5/2012, p. 831 ss.;

FOLCO-SIENA, *Il legal framework europeo di contrasto al riciclaggio transnazionale verso una svolta? Problemi attuali e prospettive di revisione organica*, in *Giurisprudenza penale web*, 2/ 2021, p. 1 ss.;

FORMICA, *Introduzione. I reati contro il patrimonio*, in VIGANÒ, PIERGALLINI (a cura di), *Reati contro la persona e contro il patrimonio*, II ed. Giappichelli, 2015, Torino, p. 323 ss.;

FORNASARI, *Il concetto di economia pubblica nel diritto penale. Spunti esegetici e prospettive di riforma*, Giuffrè, Milano, 1994;

FULVI, *La Convenzione Cybercrime e l'unificazione del diritto penale dell'informatica*, in *Dir. pen. proc.*, 5/2009, p. 639 ss.;

FUMO, *La condotta nei reati informatici*, in *Archivio Penale*, 3/2013, p. 771 ss.;

FUMO, *"Res telematica". La problematica corporeità del file ed il reato di appropriazione*, in *Rivista di diritto dei media*, 2/2020, p. 275 ss.;

FRAGASSO, VERGINE, *sub Art. 61*, in DOLCINI-GATTA, Codice penale commentato, Tomo I, V ed., 2021, p. 1230 ss.;

GABOARDI, *Le loquaci spoglie del reato continuato*, in *Cass. pen.*, 11/2014, p. 3983 ss.;

GAETA, *L'illusione della monade chiusa: primato del caso e crisi della tipicità penale*, in *Ars interpretandi* 1/2019, p. 111 ss.;

GALANTE, *Ricettazione: l'interpretazione giurisprudenziale di una fattispecie problematica*, in *Dir. pen. proc.*, 11/2017, p. 1525 ss.;

GALANTE, *La tutela penale delle carte di pagamento*, in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime,* collana *Diritto e procedura penale dell'informatica*, utet, Torino, 2019, p. 285 ss.;

GALLO, *Il dolo. Oggetto e accertamento*, Giuffrè, 1953;

GAMBARDELLA, *Il significato e il contenuto dell'avverbio fraudolentemente nel reato di false comunicazioni sociali (art. 2621, n. 1, c.c.)*, in *Cass. pen.*, 9/1998, p. 2529 ss.;

GITTI, *Emissione e circolazione di criptoattività tra tipicità e atipicità nei nuovi mercati finanziari*, in *Banca borsa e titoli di credito*, 1/2020, p. 13 ss.;

GIUDICI, *Insolvenza di un "custodial marketplace" di valute virtuali e tutela dei clienti*, in *Le Società*, 5/2020, p. 588 ss.;

GIUNTA, *Lineamenti di diritto penale dell'economia, Delitti contro l'economia pubblica e reati societari*, Vol. I., II ed., Giappichelli, 2004, Torino;

GIUNTA, *Il diritto penale dell'economia: tecniche normative e prova dei fatti*, in *Riv. trim. dir. pen. econ.*, 3-4/2017, p. 544 SS.;

GIZZI, *Inquinamento elettromagnetico e responsabilità penale: la Cassazione sul caso Radio vaticana*, in www.sistemapenale.it del 6 luglio 2011;

GRECO, *Valute virtuali e valute complementari, tra sviluppo tecnologico e incertezze regolamentari*, in *Rivista di diritto Bancario*, 1/2019, p. 61 ss.;

GROSSI, *I tormenti della "cosa mobile" penalmente rilevante: la Corte di cassazione ne estende la portata ai documenti informatici (files)*, in *Giurisprudenza penale web*, 10/2020, p. 1 ss.;

GROSSO, *Su un'interessante controversia interpretativa in tema di luogo del commesso reato e di giudice competente per territorio in materia di accesso abusivo in un sistema informatico*, in *Riv. it. dir. proc. pen.*, 2014, 1518 ss.;

GROTTO, *Regime giuridico del falso informatico e dubbi sulla funzione interpretativa dell`art. 491-bis c.p.*, in *Diritto dell'informazione e dell'informatica*, 4-5/2006, p. 589 ss.;

GUIDI, *Appropriazione, distrazione ed uso nel delitto di peculato*, Milano, 2008;

INGRAO, *Gli strumenti di prevenzione nazionali ed europei in materia di valute virtuali e riciclaggio*, in *Diritto Penale Contemporaneo Rivista trimestrale*, 2/2019, p. 159 ss.;

KROGH, *La responsabilità del gestore di piattaforme digitali per il deposito e lo scambio di criptovalute*, nota a Tribunale di Firenze, sez. fallimentare, 21 gennaio 2019, n.18, in *Diritto di Internet*, 2/2019, p. 337 ss.;

LANZI, *voce furto*, in *Enc. giur. Treccani*, vol., XIV, Roma, 1989, p. 5 ss.;

LANZI, *La difficile individuazione di limiti applicativi all'autoriciclaggio: il bene giuridico, il tempo e l'oggetto*, in *Indice penale*, 2/2017, p. 506 ss.;

LAPICCIRELLA, *voce Connessione (dir. proc. pen.),* in *Enc. Dir.*, vol. IX, 1961, p. 33 ss.;

LARINNI, *Garantismo europeista: un ossimoro? A proposito dell'accesso abusivo ad un sistema informatico o telematico (615 ter c.p.)*, in www.discrimen.it del 29 giugno 2020;

LA VATTIATA, *Brevi note "a caldo" sulla recente Proposta di Regolamento UE in tema di intelligenza artificiale,* in *www.dirittopenaleuomo.org* del 30.06.21;

LAZZONI, *la fattispecie di indebito utilizzo, falsificazione, alterazione di carte di credito e di pagamento*, in BERNASCONI, GIUNTA (a cura di), *Riciclaggio e obblighi dei professionisti*, Giuffrè, 2011, Milano, p. 189 ss.;

LEO, *Sulla qualificazione dell'utilizzo abusivo nel circuito informatico dei codici concernenti carte di credito*, in *Dir. pen. proc.*, 6/2013, p. 660 ss.;

LEPERA, *Un caso di reato semplice scambiato per reato circostanziato: sull'improbabile configurabilità dell'aggravante della "minorata difesa" in relazione alle truffe on-line*, in *Cass. pen.*, 2/2017, p. 687 ss.;

LEUCCI, *Appunti sul difficile rapporto tra linguaggio, diritto penale e tecnologia*, in *Informatica e diritto*, 2/2013, p. 151 ss.;

LIACE, *Robo-advisor e finanza comportamentale*, in FIMMANÒ, FALCONE (a cura di), *FinTech*, Edizioni scientifiche Italiane, 2019, p. 195 ss.;

LONGO, *Falso nummario e in sigilli,* in PELISSERO-BARTOLI, *Reati contro la fede pubblica*, Giappichelli, 2011, p. 11 ss.;

LONGOBARDO, *Ricettazione*, in FIORE (a cura di), *I reati contro il patrimonio*, Utet, 2010, p. 769 ss.;

LONGOBARDO, *I reati predatori contro il patrimonio*, in *Riv. it. dir. proc. pen.*, 2/2020, p. 889 ss.;

LUCANTONI, *Strumenti digitali e finanza,* in MAIMERI, MANCINI (a cura di), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale*, Quaderno di ricerca giuridica della Banca d'Italia, n. 87/2019, p.291 SS.;

LUCEV, BONCOMPAGNI, *Criptovalute e profili di rischio penale nelle attività degli exchanger*, in *Giurisprudenza Penale Web*, 3/2018, p. 1 ss.;

MAESTRI, *Lex informatica e diritto. Pratiche sociali, sovranità e fonti nel cyberspazio*, in *Ars interpretandi*, 1/2017, p. 15 ss.;

MADIA, *Considerazioni in ordine ai rapporti tra l'art. 316 ter c.p. e l'art. 640 bis: quando l'ipertrofia normativa genera disposizioni in tutto o in parte inutili*, in *Cass. pen.*, 9/2003, 2680 ss.;

MADIA, *L'impropria" incidenza della teorica del bene giuridico nel dibattito relativo alla nozione di "evento"*, in *Indice penale*, 2/2012, p. 411 ss.

MAGGIOLINO, SCOPSI, *Big data e profili di concorrenza nei mercati dei servizi bancari e finanziari*, in BOSCIA, SCHIENA, STEFANELLI (a cura di), *Digital Banking e Fin tech. L'intermediazione finanziaria tra cambiamenti tecnologici e sfide di mercato*, Bancaria editrice, 2020, p. 89 ss.;

MAGRO, *Paternalismo penale e tutela dell'investitore dal rischio finanziario*, in BORSARI, SAMMICHELI, SARRA (a cura di), *Homo Oeconomicus. Neuroscienze, razionalità decisionale ed elemento soggettivo nei reati economici*, *Ius Quid* sez. scientifica, Padova, 2015, p. 195 ss.;

MAGRO, *Truffa contrattuale e derivati: profilazione dell'investitore e standard di tutela penale*, in *Cassazione Penale*, 9/2015, p. 3355B ss.;

MAINIERI, *La Direttiva UE n. 1673/2018 sulla lotta al riciclaggio mediante il diritto penale: osservazioni sul recepimento*, nella sezione approfondimenti-antiriciclaggio di www.dirittobancario.it del 18.12.2020;

MALGIERI, *La nuova fattispecie di "indebito utilizzo d'identità digitale": un problema interpretativo*, in *Diritto Penale Contemporaneo Rivista trimestrale*, 2/2015, p. 144 ss.;

MALGIERI, *Il furto di identità digitale: una tutela patrimoniale della personalità*, in FLOR, FALCINELLI, MARCOLINI (a cura di), *La giustizia penale nella rete. Le nuove sfide della società dell'informatica nell'epoca di internet*, *I Convegno Nazionale del Laboratorio Permanente di Diritto Penale, Perugia, 19 settembre 2014*, DipLab editore, 2015, p. 37 ss.;

MANCINI, *Il furto nei supermercati: la linea di confine tra tentativo e consumazione*, in *Cass. pen.*, 3/2000, p. 608 ss.;

MANICCIA, *Gli incerti "confini" del principio di territorialità*, in *Cass. pen.*, 11/2008, p. 3717 ss.;

MANNA, *Artifici e raggiri online: La truffa contrattuale, il falso informatico e l'abuso dei mezzi di pagamento elettronici*, in *Dir. inf.*, 2002, p. 955 ss.;

MANNA, *il bene giuridico tutelato nei delitti di riciclaggio e reimpiego: dal patrimonio all'amministrazione della giustizia sino all'ordine pubblico ed all'ordine economico*, in AA. VV. (a cura di) MANNA, *Riciclaggio e Reati connessi all'intermediazione mobiliare*, Utet, 2000, p. 55 ss.;

MANGIONE, *Mercati finanziari e criminalità organizzata: spunti problematici sui recenti interventi normativi di contrasto al riciclaggio*, in *Riv. It. Dir. Proc. Pen.*, 2000, p 1102 ss.;

MANES, *Il principio di offensività nel diritto penale. Canone di politica criminale, criterio ermeneutico, parametro di ragionevolezza*, Giuffrè, Torino, 2005;

MANES, *I recenti tracciati della giurisprudenza costituzionale in materia di offensività e ragionevolezza*, in *Dir. pen. cont.*, 1/2012, 99 ss.;

MANIERI, *Quinta direttiva europea antiriciclaggio: il decreto di recepimento 125/2019 entra in vigore*, nella sezione approfondimenti di www.dirittobancario.it del 5.11.2019.;

MANTOVANI, *voce Patrimonio (reato contro il)*, in *Enc. Giur.*, vol. XXII, 1990, p. 2 ss.;

MANTOVANI, *Umanità e razionalità nel diritto penale*, Cedam, 2008;

MANTOVANI, *Diritto penale, parte speciale*, Vo. II, 7 ed, 2018;

M. MANTOVANI, *La struttura dei reati di possesso,* in www.dirittopenalecontemporaneo.it, del 7 novembre 2012;

MARGIOCCO, *Frode informatica*, in FINOCCHIARO, DELFINI (a cura di), *Diritto dell'informatica*, Assago, 2014, p. 1107 ss.;

MARINI, voce *Possesso (diritto penale)*, in *Dig. disc. pen.*, 1995, IX, 630 ss.;

MARINI, *Delitti contro il patrimonio*, Giappichelli, Torino, 1999;

MARINUCCI, *L'analogia e la "punibilità svincolata dalla conformità alla fattispecie penale"*, in *Riv. it. dir. proc. pen.*, 2007, p. 1254 ss.;

MARVULLI, *Competenza ed incompetenza penale*, in *Enc. dir.,* V agg., Milano, 2001, p. 117 ss.;

MASSI, *Speciale anti-doverosità della condotta ed elusione del fatto tipico*, Giappichelli, 2020;

MAZZANTINI, *Truffa contrattuale- La mancata restituzione del veicolo noleggiato fra truffa e appropriazione indebita*, nota a Cass. pen., Sez. VI, 12.01.2016, n. 1408, in *Giur. It.*, 7/2016, p. 1749 ss.;

MAZZANTINI, *La tutela del patrimonio alla prova della smaterializzazione dei rapporti socio-economici. La centralità dei delitti di frode nel sistema penale "vivente"*, in *Riv. it. dir. pen. proc.*, 1/2020, p. 75 ss.

MENZELLA, *Il ruolo dei big data e il mobile payment*, in MAIMERI, MANCINI (a cura di), *Le nuove frontiere dei servizi bancari e di pagamento fra PSD 2, criptovalute e rivoluzione digitale*, Quaderno di ricerca giuridica della Banca d'Italia, n. 87/2019, p. 143 ss.;

MERLI, *Introduzione alla teoria generale del bene giuridico. Il problema. Le fonti. Le tecniche di tutela penale*, ESI, Napoli, 2006;

MICHELETTI, *Reato e territorio*, in *Criminalia*, 2009, p. 565 ss.;

MICHELETTI, J*us contra lex. Un campionario dell'incontenibile avversione del Giudice penale per la legalità*, in *Criminalia*, 2016, p. 161 ss.;

MIGLIONICO, *Innovazione tecnologica e digitalizzazione dei rapporti finanziari*, in *Contratto e Impr.*, 4/2019, p. 1376 ss.;

MILITELLO, *voce Patrimonio (delitti contro)*, in *Digesto delle discipline penalistiche*, IX, Torino, 1995, p. 3 ss.;

MILITELLO, *L'identità della scienza giuridica penale nell'ordinamento multilivello*, in *Riv. It. Dir. Proc. Pen.*, 1/2014, p. 106 ss.;

MILONE, *La tutela dell'identità digitale nella nuova circostanza aggravante del delitto di frode informatica*, in *Legislazione penale*, 1-2/2014, p. 133 ss.;

MINAFRA, *Le caratteristiche delle criptovalute e il loro utilizzo a fini illeciti: profili sostanziali e processuali*, in CASSANO, DI CIOMMO, DE RITIS (a cura di), *Banche, Intermediari e Fintech, Nuovi strumenti digitali in ambito finanziario*, Giuffrè, 2021, p. 517 ss.;

MINICUCCI, *Le frodi informatiche*, in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime*, collana *Diritto e procedura penale dell'informatica*, utet, Torino, 2019, p. 827 ss.;

MINNITI, *Il momento consumativo della truffa realizzata mediante pagamento con bonifico bancario*, nota a Cass. pen., sez. fer., 30.08.2016, n.37400, in *Ilpenalista.it* del 10.11.2016;

MOCCIA, *Tutela penale del patrimonio e principi costituzionali*, Padova, 1988, p. 62 ss.;

MOCCIA, *Impiego di capitali illeciti e riciclaggio: la risposta del sistema penale italiano*, in *Riv. It. Dir. Proc. Pen.*, 1995, p. 728 ss;

MOMOT, TESLENKO, TUMIETTO, *Blockchain e DLT per la pubblica utilità: gli esempi più promettenti e i problemi da risolvere*, in www.agendadigitale.eu del 28 gennaio 2019;

MONGILLO, *Il principio di offensività tra costituzionalizzazione e codificazione*, in *Giur. mer.*, 2002, p. 1144 ss.;

MONGILLO, *Il contrasto alla corruzione tra suggestioni del "tipo d'autore" e derive emergenziali*, in *Riv. It. Dir. Proc. Pen.*, 2/2020, p. 967 ss.;

MORERA, *Consulenza finanziaria e robo-advisor: profili cognitivi*, in FIMMANÒ, FALCONE (a cura di), *FinTech*, Edizioni scientifiche Italiane, 2019, p. 203 ss.;

MORGANTE, *Riflessione su taluni profili problematici dei rapporti tra fattispecie aventi ad oggetto operazioni su denaro o beni di provenienza illecita*, in *Cass. pen.* 1998, p. 2511 ss;

MORGANTE, *Note critiche in tema di illiceità espressa e speciale*, in DE FRANCESCO (a cura di), *Scritti in onore di Antonio Cristiani*, 2002, p. 569 ss.;

MORGANTE, *L'illiceità speciale nella teoria del reato*, Torino, 2002;

MORGANTE, *Il reato come elemento del reato. Analisi e classificazione del concetto di reato richiamato dalla fattispecie penale*, Giappichelli, 2013;

MORGANTE, AMORE, DI VETTA, FIORINELLI, GALLI, *Enforcement e regimi sanzionatori tra rischi per la clientela e vincoli per gli operatori: i profili penalistici*, in CONSOB (a cura di), *Il FinTech e l'economia dei dati. Considerazioni su alcuni profili civilistici e penalistici. Le soluzioni del diritto vigente ai rischi per la clientela e gli operatori*, nella collana *Quaderni FinTech* n. 2/2018, p. 47 ss.;

MORGANTE, FIORINELLI, *Sul diritto penale delle relazioni negoziali complesse: la tutela della parte "vulnerabile" tra contratto e mercato*, in *www.discrimen.it* del 24.6.20;

MUCCIARELLI, *Commento all'art. 10 della l. 23/12/1993 n. 547*, in *Legislazione Penale*, 1996, p. 57 ss.;

NADDEO, *Nuove frontiere del risparmio, Bitcoin Exchange e rischio penale*, in *Dir. pen. proc.*, 1/2019, p. 101 ss.;

ONORATI, COZZA, *I reati in tema di comunicazioni*, in PARODI, SELLAROLI (a cura di), *Diritto penale dell'informatica. Reati della rete e sulla rete*, Giuffrè, 2020, p. 361 ss.;

ORLANDO, *Mobilità dei reati nello spazio transfrontaliero e nuovi confini delle norme penali: verso una giurisdizione "a geometria variabile"?*, in MILITELLO, SPENA (a cura di), *Mobilità, sicurezza e nuove frontiere tecnologiche*, Giappichelli, 2018, p. 79 ss.;

PACILLO, *Le valute virtuali alla luce della V Direttiva Antiriciclaggio*, in *Rivista trimestrale di diritto tributario*, 3-4/2018, n., p. 631 ss.;

PAGLIARO, *voce Concorso di reati*, in *Enc. Dir.*, vol. VIII, Milano, 1961, p. 660 SS.;

PAGLIARO, voce *Appropriazione indebita,* in *Dig. Disc. pen.*, I, 1987,p. 227 ss.;.

PAGLIARO, *il reato*, Giuffrè, Milano, 2007;

PALAVERA, *Beni comuni e sistema penale*, in *disCrimen* dal 23.6.2021;

PALMIERI, *La prevalenza di interessi patrimoniali nella disciplina del riciclaggio e la punibilità dell'autoriciclaggio come simbolica incriminazione del bis in eadem*, in *Indice penale*, 1/2016, n. 1, p. 57 ss.;

B. PANATTONI, *I riflessi penali del perdurare nel tempo dei contenuti illeciti nel cyberspace*, in www.sistemapenale.it del 22 maggio 2020;

PANEBIANCO, *La persistente vivacità del reato continuato nella giurisprudenza delle Sezioni Unite*, in *Giur. it.*, marzo 2019, p. 688 ss.;

PAOLONI, *Il momento consumativo del delitto di appropriazione indebita,* nota a Cass. pen. sez. II, 10.04.2014, n.17901, in *Cass. pen.*, 4/2015, p. 1449 ss.;

PAONESSA, *Gli obblighi di tutela penale La discrezionalità legislativa nella cornice dei vincoli costituzionali e comunitari,* Firenze, 2009, p. 237 ss.;

PAONESSA, *Parola e linguaggio nel diritto penale: la garanzia della forma oltre il formalismo*, in *Studi Senesi*, vol. CXXIX, p. 303 ss.;

PAPA, *Future crimes: intelligenza artificiale e rinnovamento del diritto penale*, in *www.discrimen.it* del 4.3.2020;

PAPA, *Fantastic Voyage. Attraverso la specialità del diritto penale*, Giappichelli, 2019;

PAPA, *La tipicità iconografica della fattispecie e l'interpretazione del Giudice. La Tradizione illuministica e le sfide del presente*, in CONTE, LANDINI (a cura di), *Principi, regole, interpretazione. Contratti e obbligazioni, famiglie e successioni. Scritti in onore di Giovanni Furgiuele*, 2017, p. 329 ss.;

PARODI, *La frode informatica: presente e futuro delle applicazioni criminali nell'uso del software*, in *Dir. pen. proc., 12*/1997, p. 1538 SS.;

PARODI, *Riciclaggio e monete elettroniche: le nuove indicazioni del d.lgs. 125/2019*, in www.llpenalista.it del 28 novembre 2019;

PARODI, LOMBARDO, GHIRARDI, *Il riciclaggio e l'aggiotaggio telematico*, in PARODI, SELLAROLI (a cura di), *Diritto penale dell'informatica. Reati della rete e sulla rete*, Giuffrè, 2020, p. 445 ss.;

PASCALE, *Circostanze-Il concorso tra più circostanze tipizzate al n. 1, 3° comma dell'art. 628 c.p.*, nota a Cass. pen., sez. II, 09.10.2020, n. 29792, in *Giur. It.*, 5/2021, p. 1196 ss.;

PECORELLA, voce *Ricettazione*, in *NN.D.I.*, XV, 1968, p. 924 ss.;

PECORELLA, voce *Furto*, in *Enc. dir.*, XVIII, 1969, p. 313 ss.;

PECORELLA, *Circolazione del denaro e riciclaggio,* in *Riv. It. dir. Proc. Pen., 1991, p. 1221 ss.;*

C. PECORELLA, *Il nuovo diritto penale delle «carte di pagamento», Il nuovo diritto penale delle "carte di pagamento"*, in *Riv. it. dir. proc. pen.*, 1993, p. 239 ss.;

C. PECORELLA, *Diritto penale dell'informatica*, II ed., Padova, 2006;

C. PECORELLA, *Truffe on line: momento consumativo e competenza territoriale, "Alcune considerazioni sul momento consumativo della truffa)*, in *Riv. it. dir. e proc. pen*., 2012 p. 799 ss.;

C. PECORELLA, *L'attesa pronuncia delle sezioni unite sull'acceso abusivo a un sistema informatico: un passo avanti non risolutivo*, in *Cass. pen*., 2012, 3681 ss.;

C. PECORELLA, DOVA, *Profili penali delle truffe on line*, in *Arch. Pen*., 3/2013, 799 ss.;

C. PECORELLA, *sub art. 615 quater*, in DOLCINI-GATTA, *Codice penale commentato*, Tomo III, V ed., 2021, p. 2072 ss.;

C. PECORELLA *sub art. 617 quinquies c.p.*; in DOLCINI-GATTA, *Codice penale commentato*, Tomo III, V ed., 2021,p. 2148 ss.;

C. PECORELLA, *sub art. 640 ter c.p.*, in DOLCINI-GATTA (a cura di), *Codice Penale Commentato*, Tomo III, V ed., 2021, p. 2660 ss.;

PEDRAZZI, *Inganno ed errore nei delitti contro il patrimonio*, Giuffrè, 1955;

PEDRAZZI, *Mercati finanziari (disciplina penale),* in *Dig. Disc. Pen.,* Vol. VII, Torino, 1993, p. 654 ss.;

PEDRAZZI, *La riforma dei reati contro il patrimonio e contro l'economia, in AA.VV., Verso un nuovo codice penale. Itinerari. Problemi. Prospettive, Atti del Convegno di Palermo del 7-10 novembre 1991*, Milano, 1993, p. 350 ss.;

PEDRAZZI, voce *Appropriazione indebita*, in *Enc. dir*., vol. II, Milano, 1958, p. 833 ss.;

PEDULLÀ, *Osservazioni a Cass. Pen., sez. V, data udienza Ud. 12 gennaio 2018, data deposito (dep. 20 aprile 2018), n. 17923*, in *Cass. pen.,* 10/2018, p. 3209 ss.;

PELISSERO, *Truffa aggravata per il conseguimento di erogazioni pubbliche*, in *Riv. it. dir. proc. pen*., 1991, p. 923 ss.;

PERNICE, *Criptovalue e bitcoin,* in FIMMANÒ, FALCONE (a cura di), *FinTech,* Edizioni scientifiche Italiane, 2019, p. 491 ss.;

PIANCASTELLI, *La ricezione di somme di denaro provento di phishing: risultanze investigative e problemi applicativi in punto di qualificazione giuridica*, in *www.dirittopenalecontemporaneo.it*, 3 marzo 2015;

PICCINNI, *I delitti contro la fede pubblica e la responsabilità amministrativa delle persone giuridiche e delle società alla luce dell'articolo 25 bis del d.lgs.231/2001*, in *Interventi-Rivista 231*, gennaio 2016;

PICOTTI, *Studi di diritto penale dell'informatica*, Tipogr. Godo, Verona, 1992;

PICOTTI, *Il dolo specifico. Un'indagine sugli "elementi finalistici" delle fattispecie penali*, Giuffrè, 1993;

PICOTTI, *Reati Informatici,* in *Enc. giur. Treccani, Aggiornamento, VIII,* Roma, 2000, p. 2 ss.;

PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, Cedam, 2004;

PICOTTI, *L'attuazione in Italia degli strumenti dell'Unione europea per la protezione penale degli interessi finanziari comunitari*, in *Riv. trim. dir. pen. econ*., 3/2006, p. 615 ss.;

PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. pen. proc.*, 6/2008, p. 700 ss.;

PICOTTI, *Limiti garantistici delle incriminazioni penali e nuove competenze europee alla luce del Trattato di Lisbona*, in GRASSO, PICOTTI, SICURELLA (a cura di), *L'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona*, Milano, 2011, p. 207 ss.;

PICOTTI, *Le basi giuridiche per l'introduzione di norme penali comuni relativi ai reati oggetto della competenza della procura europea*, in GRASSO, ILLUMINATI, SICURELLA, ALLEGREZZA (a cura di), *Le sfide dell'attuazione di una Procura europea. Definizione di regole comuni e loro impatto sugli ordinamenti interni*, Milano, 2013, p. 65 ss.;

PICOTTI, *Profili penali del cyberlaundering: le nuove tecniche di riciclaggio*, in *Riv. Trim. dir. pen. ec.*, 3-4/2018, p. 590 ss.;

PICOTTI, VADALÀ, *Sicurezza cibernetica: una nuova fattispecie delittuosa a più condotte con estensione della responsabilità degli enti*, in www.sistemapenale.it, 5 dicembre 2019;

PICOTTI, *Diritto penale e tecnologie informatiche: una visione d'insieme,* in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime,* collana *Diritto e procedura penale dell'informatica*, utet, Torino, 2019, p. 35 SS.;

PICOTTI, *Cybersecurity: quid novi?,* in *Diritto di Internet*, 1/2020, p. 11 ss.;

PICOTTI, *New technologies as tool and means against crime: substantive aspects*, in SEVERINO, VERVAELE, GULLO (a cura di), *Criminal Justice and Corporate Business, 20th AIDP International Congress of Penal Law, Rome, Italy, 13th-16th November 2019*, Muklu Publishers, 2021, p. 183 ss.;

PIERGALLINI, "*Civile" e "penale" a perenne confronto: l'appuntamento di inizio millennio*, in *Riv. it. dir. e proc. pen.*, 4/2012, p. 1299 ss.;

PIERGALLINI, *Intelligenza Artificiale: da 'mezzo' ad 'autore' del reato?*, in *Riv. it. dir. proc. pen.*, 4/2020, p. 1743 ss.;

PIOLETTI, *Lex mercatoria e diritto penale*, in *Indice penale*, 2/2017, p. 478 ss.;

PIRANI, *Gli strumenti della finanza disintermediata: Initial Coin Offering e blockchain, in Analisi Giuridica dell'Economia*, 1/2019, p. 327 ss.;

PISANI, *La nozione di "cosa mobile" agli effetti penali e i files informatici: il significato letterale come argine all'applicazione analogica delle norme penali,* in *Dir. pen. proc.,* 5/2020, p. 651 ss.;

PISTORELLI, *Prime note sulla legge di conversione, con modificazioni, del d.l. n. 93 del 2013, in materia tra l'altro di "violenza di genere" e di reati che coinvolgano minori*, in www.dirittopenalecontemporaneo.it;

PLANTAMURA, *Tipo d'autore o bene giuridico per l'interpretazione e la riforma del delitto di riciclaggio?*, in *Riv. Trim. dir. Pen. econ.*, 1-2/2009, p. 161 ss.;

PLANTAMURA, *La tutela penale delle comunicazioni informatiche e telematiche*, in *Dir. informatica*, 6/2006, p. 847 ss.;

POERIO, *Possesso*, in *Studium iuris*, n. 12/2001, p. 1546 ss.;

PONTEPRINO, *La "dubbia" configurabilità dell'appropriazione indebita d'uso*, in *Dir. pen. proc.*, n. 1/2021, p. 87 ss.;

PROSDOCIMI, *Profili penali del post fatto,* Giuffrè, 1982;

PROSDOCIMI, *Concorso di reati e di pene*, in *Digesto disc. pen.*, vol. II, Torino, 1988, 508 ss.;

PULITANÒ, *Principio di legalità ed interpretazione della legge penale*, in COCCO (a cura di), *Interpretazione e precedente giudiziale in diritto penale*, Padova, 2005, p. 27 ss.;

RAMPIONI, *Diritto penale dell'economia*, Giappichelli, Torino, 2016;

RAMPONE, "*Smart contract*": *né* "*smart*", *né* "*contract*", in *Rivista di diritto privato*, 2/2020, p. 241 ss..;

REINOTTI, voce *Ricettazione e riciclaggio*, in *Enc. dir.*, vol. XL, 1989, p. 461 ss.;

REMOTTI, *Blockchain smart contract. Un primo inquadramento, in Osservatorio del diritto civile e commerciale*, 1/2020, p. 189 ss.;

RESTA, *Cybercrime e cooperazione internazionale, nell'ultima legge della legislatura,* in *Giur. merito*, 9/2008, p. 2147 ss.;

RESTA, *Il delitto di furto. Profili sostanziali e strategie processuali alla luce delle più recenti evoluzioni normative,* Cedam, 2010;

RINALDI, *Approcci normativi e qualificazione giuridica delle criptomonete*, in *Contratto e Impresa*, 1/2019, p. 257 ss.;

RISICATO, *Gli elementi normativi della fattispecie penale, Profili generali e problemi applicativi,* Giuffrè, 2004;

RISICATO, *Diritto alla sicurezza e sicurezza dei diritti: un ossimoro invincibile?*, Giappichelli, 2019;

ROCCO, *L'oggetto del reato e della tutela giuridica penale*, 1913;

ROMOLOTTI, *Cybersecurity: un ponte tra GDPR e d.lgs. 231/2001 alla luce del d.lgs. 101/2018*, in *La responsabilità amministrativa della società e degli enti*, 2/2019, p. 71 ss.;

ROMOLOTTI, *Il decreto Cybersecurity e le nuove ipotesi rilevanti di reato ex d.lgs. 231/2001,* in *La responsabilità amministrativa della società e degli enti*, 2/20, p. 121 ss.;

ROSATO, *Profili Penali della criptovalute*, *Quaderni del Centro Ricerca Sicurezza e Terrorismo*, Pacini Giuridica, 2012;

ROSSI, *L'esperienza giurisprudenziale del diritto penale economico nel tempo della crisi,* in *Riv. it. dir. e proc. pen.,* 2/2014, p. 627 ss.;

RUEDA MARTÌN, *La confidencialidad, integridad y disponibilidad de los sistemas de información como bien jurídico protegido en los delitos contra los sistemas de información en el código penal español,* in *Diritto penale contemporaneo Rivista trimestrale*, 3/2020, p. 199 ss.;

RUGGIERO, *Momento consumativo del reato e conflitti di giurisdizione nel ciberspazio*, in *Giur. merito*, 2002, p. 254 ss.;

SALCUNI, *Le falsità informatiche*, in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime*, collana *Diritto e procedura penale dell'informatica*, utet, Torino, 2019, p. 273 ss.;

SALVADORI, *Quando un insider accede abusivamente ad un sistema informatico o telematico? Le Sezioni Unite precisano l'ambito di applicazione dell'art. 615 ter c.p.*, in *Riv. trim. dir. pen. econ.*, 1-2/2012, p. 369 ss.;

SALVADORI, *I reati di possesso. Un'indagine dogmatica e politico-criminale in prospettiva storica e comparata*, Edizioni Scientifiche Italiane, Napoli, 2016;

SALVADORI, *Criminalità informatica e tecniche di anticipazione della tutela penale. L'incriminazione dei "dual-use software"*, in *Riv.it. di dir. e proc. pen.*, 2/2017, p. 747 ss..

SALVADORI, *I reati contro la riservatezza informatica*, in CADOPPI, CANESTRARI, MANNA, PAPA (a cura di), *Cybercrime*, collana *Diritto e procedura penale dell'informatica*, utet, Torino, 2019, p. 656 ss.;

SANTORIELLO, *I reati informatici dopo le modifiche apportate dalla legge 48/2008 e la responsabilità degli enti*, in *La Responsabilità amministrativa delle società e degli enti*, 1/2011, p. 211 ss.;

SARZANA DI S. IPPOLITO, *Blockchain e smart contract nel nuovo Decreto Semplificazioni,* in *Diritto di internet*, 1/2019, p. 17 ss.;

SCALIA, *Relazioni pericolose nel "terzo spazio"*, in *Diritto Penale Uomo,* 1/2021, p. 109 ss.;

SCARCELLA, *Il phishing è punibile come frode informatica*, in *Quotidiano Giuridico* del 13.11.2018;

SCARCELLA, *L'uso dei codici di una carta di credito, senza possesso della stessa, non è frode informatica*, in *Quotidiano Giuridico* del 16.1.2019;

SCHILLACI, *Sulla competenza per territorio nel reato di truffa online compiuto mediante accredito su carta postepay*, nota a Cass. pen., sez. II, 06.06.2019, n.49195, in *Ilpenalista.it* del 29.05.2020;

SCOPINARO, *Acquisto e utilizzo illecito di carta di credito via internet*, nota a Cass. Sez. I, 5-11-2002 n. 37115, in *Dir. pen. proc.*, 6/2003, p. 725 ss.;

SCOPINARO, *Furto di dati e frode informatica*, in *Dir. pen. proc.*, 3/2007, p. 363 ss.,

SCOPINARO, *Internet e reati contro il patrimonio*, Giappichelli, 2007;

SCUTO, *La tutela costituzionale del risparmio negli anni della crisi economica*, in *www.federalismi.it* del 25 ottobre 2019;

SEMINARA, *I soggetti attivi del reato di riciclaggio tra diritto vigente e proposte di riforma*, in *Dir. pen. proc.*, 2005, p. 241 ss;

SEMINARA, *Locus commissi delicti, giurisdizione e competenza nel cyberspazio,* relazione al Convegno "*Presi nella rete – Analisi e contrasto della criminalità informatica*", Pavia, 23 novembre 2012, reperibile su *www.informaticagiuridica.unipv.it/convegni/2012/SEMINARA*;

SEMINARA, *Note sul reato di accesso abusivo a sistemi informatici o telematici da parte di un pubblico agente (art. 615-ter, c. 2, n. 1, c.p.)*, in *Rivista di diritto dei media*, 2/2018, p. 1 SS.;

SERAFIN, *FinTech: tra piattaforme di crowdfunding, valute virtuali e contrasto del riciclaggio*, in *Ricerche giuridiche*, vol. 8, 1/2019, p. 119 ss.;

SERRA, *Interpretazione estensiva vs divieto di analogia: una problematica tradizionale in una recente (e criticabile) pronuncia della Corte di Cassazione*, in *Diritto penale contemporaneo Rivista trimestrale*, 6/2018, p. 137 ss.;

SEVERINO, *Sicurezza dei mercati finanziaria: interessi tutelati e strumenti di tutela,* in *Riv. it. dir. e proc. pen.*, 2/2014, p. 672 ss.;

SGUBBI, voce *Patrimonio (reati contro il),* in *Enc. Giur.*,XXXII, 1982, p. 331 ss.;

SGUBBI, *Il reato come rischio sociale. Ricerche sulle scelte di allocazione dell'illegalità penale*, il Mulino, Bologna, 1990;

SCHENA, TANDA, *Linee evolutive della regolamentazione e della vigilanza sull'innovazione finanziaria digitale*, in BOSCIA, SCHIENA, STEFANELLI (a cura di), *Digital Banking e Fin tech. L'intermediazione finanziaria tra cambiamenti tecnologici e sfide di mercato*, Bancaria editrice, 2020, p. 69 ss.;

SCHENA, TANDA, ARLOTTA, *Lo sviluppo del FinTech. Opportunità e rischi per l'industria finanziaria nell'era digitale*, in *Quaderno Fin Tech*, 1/2018, p. 1 ss.;

SICIGNANO, *Bitcoin e riciclaggio*, Giappichelli, Torino, 2019;

SICIGNANO, *Gli obblighi antiriciclaggio degli operatori in moneta virtuale: verso l'autocertificazione per gli utenti della blockchain?*, in *Diritto Penale Contemporaneo Rivista trimestrale*, 4/2020, p. 146 ss.;

SICCARDI, *Il "fine di profitto" nei delitti contro il patrimonio*, in *Dir. pen. proc.*, 3/2016, p. 358 ss.;

SINISCALCO, voce *Locus commissi delicti*, in *Enc. dir.*, vol. XXIV, 1974, p. 1051 ss.;

SOLA, *Tutela dei beni immateriali e reati contro il patrimonio: alcune osservazioni*, in *Ind. Pen.*, 1990, p. 782 ss.;

SOTIS, *Il ''concorso materiale apparente'': confine tra artt. 15 e 81 c.p.*, in *Giur. it.*, gennaio 2020, p. 187 ss.;

SPINA, *Nuove norme in materia di tutela penale dell'euro*, in *www.legislazionepenale.eu* del 27 dicembre 2016;

TAMBURRO, *Il bene giuridico protetto dal reato di furto: una questione anche di 'possesso'*, in *Rivista penale*, 6/2014, p. 551 ss.;

TERRACINA, *La truffa aggravata per il conseguimento di erogazioni pubbliche ed il ruolo del bene giuridico nella fattispecie di reato*, in *Indice penale*, 2/2003, p. 667 SS.;

TESTA, *Appropriazione indebita*, in FIORE (a cura di), *I reati contro il patrimonio*, Utet, 2010, p. 323 ss.;

TRABACCHI, *I delitti contro la fede pubblica,* in MARINUCCI-DOLCINI (a cura di), *Trattato di diritto penale. Parte speciale*, Padova, 2011;

TUZET, *La storia infinita ancora su analogia e interpretazione estensiva*, in *Criminalia*, 2011, p. 507 ss.;

URBANI, *La disciplina antiriciclaggio alla prova del processo di digitalizzazione dei pagamenti*, in *Rivista di diritto bancario*, 5/2018, p. 1 ss.;

VADALÀ, *L'autoriciclaggio e la soluzione italiana nella recente riforma*, in *Riv. Trim. dir. Pen. Econ.*, 3-2015, p. 1916 ss.;

VADALÀ, *La provenienza illecita nel delitto di riciclaggio: possibili novità dalla quarta direttiva antiriciclaggio*, in *Riv. Trim. dir. Pen. Econ.*, 1-2 2017, p. 234 ss ;

VADALÀ, *La disciplina sugli usi e abusi delle valute virtuali*, in *Diritto di Internet*, 3/2020, p. 397 ss.;

VADALÀ, *Criptovalute e cyberlaundering: novità antiriciclaggio nell'attesa del recepimento della Direttiva (UE) 2018/1673 sulla lotta al riciclaggio mediante il diritto penale*, in *www.sistemapenale.it* del 6 maggio 2020;

VADALÀ, *La dimensione finanziaria delle valute virtuali. Profili assiologici di tutela penale*, in *Giur. it.*, 10/21, p. 2224 ss.;

VALLINI, *La sottrazione violenta di ovociti e le torsioni del "tipo criminoso"*, in *Giur. It.*, 7/2021, p. 1732 ss.;

VASSALLI, *Il contributo di Filippo Grispigni alla teoria dell'elemento oggettivo del reato*, in *La Scuola positiva*, 1956, p. 367 ss.;

VASSALLI, voce *Antefatto non punibile, post-fatto non punibile*, in *Enc. Dir.*, vol. II, 1958, p. 507 ss.,

VASSALLI, *Le norme penali a più fattispecie e l'interpretazione della legge Merlin*, in *Studi in onore di F. Antolisei*, III, Giuffrè, 1965, 153 ss.;

VASSALLI, voce *Progressione criminosa e reato progressivo*, in *Enc. Dir.*, vol. XXXVI, 1987, p. 1150 ss.;

VASSALLI, voce *Analogia nel diritto penale*, in *Dig. disc. pen.*, vol. I, Torino, 1987, 158 ss.;

VILLONI, *Una strategia europea contro il crimine organizzato: la decisione quadro del Consiglio dell'Unione Europea relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti*, in *Giur. merito*, 1/2002, p. 263 ss.;

VINCIGUERRA, *Due anni alla commissione ministeriale per la riforma del codice penale. Un consuntivo*, in *Dir. pen. XXI secolo*, 2004, 103 ss.;

VISCONTI, *La valutazione delle blockchain: internet of value, network digitali e smart transaction,* in *Il Diritto Industriale*, 3/2019, p. 301 ss.;

VITALE, *Brevi riflessioni sul reato di "frode informatica": i servizi a contenuto applicati dalle compagnie telefoniche nell'alveo dei cybercrime*, in *Archivio Penale*, 1/2015, p. 4 ss.;

ZACCAGNINI, *Note sull'art. 12 della l. n. 197/91, quale "disposizione di chiusura" della normativa di compliance italiana e suoi rapporti con il delitto di ricettazione*, in *Cass. pen.*, 1/2002, p. 318 ss.;

ZAGREBELSKI, *voce Reato continuato*, in *Enc. Dir.*, vol. XXXVIII, Milano, 1987, p. 839 ss.;

ZANCHETTI, *Il riciclaggio di denaro proveniente da reato,* Giuffre, Milano, 1997;

ZANNOTTI, *Appropriazione indebita di "files"? Il "file", come l'aria, è un bene immateriale che può essere concretizzato solo attraverso un supporto*, in *La Giustizia Penale*, 8-9/2020, fasc. 8-9, p. 464 ss.;

ZATTI, *La dimensione costituzionale della tutela del risparmio. Dalla tutela del risparmio alla protezione dei risparmiatori/investitori e ritorno?,* in *Forum di quaderni costituzionale rassegna*, 2010, p. 1 ss.;

ZICCARDI, *Furto d'identità,* in *Dig. Disc. pen.*, VI, agg., Torino, 2001, p. 253 ss.;

ZONILE, *La regolamentazione internazionale ed europea di contrasto all'uso di valute virtuali da parte della criminalità transnazionale*, in *Rivista di Diritto Internazionale*, 1/2019, p. 137 SS.;

ZUCCALÀ, *Due questioni attuali sul bene giuridico: la pretesa dimensione "critica" del bene e la pretesa necessaria offesa ad un bene*, in *Riv. trim. dir. pen. econ.*, 3-4/2004, p. 839 ss.;

ZUFFADA, *Giornalismo d'inchiesta e diritto penale: la Corte di cassazione apre le porte alla configurabilità della scriminante del diritto di cronaca rispetto al reato di ricettazione commesso dal giornalista*, in *www.sistemapenale.it* del 19 marzo 2020.

Sull'Autrice

Docente a contratto per l'insegnamento "*Cybercrime*" del corso di laurea Data science della Scuola di Scienze e Ingegneria dell'Università degli studi di Verona.

Assegnista di ricerca sul tema "*Nuove tecnologie e reati in materia economicofinanziaria: dal cyberlaundering alle frodi negli strumenti di pagamento elettronici e nell'accesso del credito*", del Centro IUSTec, struttura istituita nel contesto del Progetto di Eccellenza 2018-2022 del Dipartimento di Scienze Giuridiche dell'Università di Verona.

Membro del team dell'Osservatorio Cybercrime del Dipartimento di Scienze Giuridiche dell'Università di Verona, Direttore Scientifico Prof. Lorenzo Picotti. È co-curatrice della relativa rassegna mensile on line di novità legislative, giurisprudenziali e dottrinali sulle tematiche delle criminalità informatica e di quella bimestrale Cybercrime di novità in materia di diritto e processo penale e nuove tecnologie, che viene realizzata e pubblicata in collaborazione con Sistema Penale, rivista nazionale on line di riferimento sui temi relativi al diritto e alla giustizia penale.

Ha partecipato al progetto "*Rischio, governance e responsabilità nei settori dell'edilizia e dell'agricoltura nell'area veneta*" finanziato dalla Fondazione Cariverona, con un incarico di collaborazione, assegnatole dal Dipartimento di Scienze Giuridiche dell'Università di Verona, per la realizzazione di un'indagine relativa all'implementazione della disciplina del whistleblowing "privato" da parte soprattutto delle medie e piccole imprese venete dei settori coinvolti nel progetto di ricerca.

Dottore di ricerca presso l'Università degli studi di Verona in "*Diritto ed Economia dell'Impresa. Discipline interne ed internazionali*" con una tesi su "*Riciclaggio: repressione, prevenzione e prospettive di riforma*"- Relatore il Prof. Lorenzo Picotti.

Avvocato iscritto dal 2013 all'Ordine degli Avvocati di Verona.

Collabora stabilmente con le cattedre degli insegnamenti di diritto penale del Dipartimento di Scienze Giuridiche dell'Università di Verona.

È autrice di diverse pubblicazioni scientifiche sui temi della criminalità economica ed informatica.

*Con il volume **"La tutela penale della sicurezza degli scambi economici digitali"** si è verificata, attraverso la "lente" delle valute virtuali, la capacità delle tecniche d'incriminazione dei delitti contro il patrimonio, sia tradizionali che informatici, di tenere il passo della digitalizzazione del sistema economico.*

Non si è trattato semplicemente di rintracciare le possibili fattispecie applicabili, evidenziandone i limiti e proponendone le modifiche ritenuto opportune, ma d'individuare paradigmi punitivi che potessero fungere da indicazioni per un inquadramento sistematico della tutela penale degli scambi digitali.

All'esito dell'indagine è emerso come la dematerializzazione non determina una modifica radicale del modo d'intendere il patrimonio, ma l'emersione di esigenze di tutela penale ulteriori, direttamente discendenti dalla dimensione digitale che esso assume e riferibili -in una chiave dogmatica nuova- alla sicurezza informatica.

La portata unificante della cybersecurity va, in particolare, oltre la mera sommatoria "cumulativa" di interessi eterogenei, operando in chiave unitaria di "contesto tecnocratico" e globale: la tutela d'interessi individuali, come quelli patrimoniali, è dipendente dall'interazione delle regole giuridiche con quelle tecniche che governano i sistemi e le strutture informatiche e il cui rispetto è necessario per il corretto funzionamento di questi ultimi.