Quaderni della rivista di diritto privato

ISBN 979-12-5965-348-2

€ 22,00

F. Borgia e B. Sirgiovanni (a cura di) Intelligenza artificiale e diritto: la cripto-arte e la sua circolazione

Quaderni della rivista di diritto privato

Intelligenza artificiale e diritto: la cripto-arte e la sua circolazione

Un dialogo interdisciplinare

a cura di
Fiammetta Borgia e Benedetta Sirgiovanni

CACUCCI EDITORE
BARI

Il volume raccoglie i risultati della ricerca interdisciplinare triennale (2021-2023): "Cripto arte: inquadramento giuridico e problemi di circolazione nell'ordinamento interno e internazionale", culminato con il Convegno: "Intelligenza artificiale e diritto: la criptoarte e la sua circolazione. Un dialogo interdisciplinare", tenutosi, l'8 maggio 2023, presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Roma Tor Vergata, Sede didattica del Foro Italico.

Gli Autori

Fiammetta Borgia, *Professore associato di Diritto internazionale presso l'Università degli studi di Roma Tor Vergata*

Gianluca Contaldi, *Professore ordinario di Diritto dell'Unione europea presso l'Università degli studi di Macerata*

Giampaolo Frezza, *Professore ordinario di Diritto civile presso l'Università Lumsa di Palermo*

Enrico Gabrielli, *Professore ordinario di Diritto civile presso l'Università degli studi di Roma Tor Vergata*

Edoardo Marcenaro, *Curatore e collezionista d'arte*

Fabrizio Marongiu Buonaiuti, *Professore ordinario di Diritto internazionale presso l'Università degli studi di Macerata*

Stefano Preziosi, *Professore ordinario di Diritto penale presso l'Università degli studi di Roma Tor Vergata*

Vincenzo Ricciuto, *Professore ordinario di Diritto privato presso l'Università degli studi di Roma Tor Vergata*

Benedetta Sirgiovanni, *Professore associato di Diritto privato presso l'Università degli studi di Roma Tor Vergata*

Quaderni della rivista di
diritto privato

Intelligenza artificiale e diritto: la cripto-arte e la sua circolazione

Un dialogo interdisciplinare

a cura di
Fiammetta Borgia e Benedetta Sirgiovanni

CACUCCI EDITORE
BARI

Quaderni della rivista di diritto privato

CRITERI DI SELEZIONE DEI VOLUMI PUBBLICATI

La valutazione di tutti i contributi oggetto di pubblicazione viene effettuata in totale anonimato secondo il sistema "*double blind*", in osservanza di quanto prevede il Regolamento ANVUR, da un soggetto terzo, di volta in volta, individuato dalla Direzione, secondo le sue specifiche competenze nelle aree tematiche di pertinenza del contributo sottoposto a valutazione nell'ambito del Comitato di Valutazione composto da soggetti autonomi rispetto agli Organi della Rivista. Solo in casi eccezionali la Direzione assume direttamente la responsabilità della pubblicazione segnalando la circostanza e le relative motivazioni in una nota nella prima pagina del contributo.
L'Autore di uno scritto che aspiri ad essere pubblicato in questi Quaderni deve inviare il proprio lavoro alla Redazione, la quale svolgerà un esame preliminare concernente:
– la attualità del contributo;
– la pertinenza dell'argomento oggetto del contributo con le materie trattate dai Quaderni.
In caso di accettazione del contributo per la sottoposizione alla procedura di referaggio, il Direttore, o un componente della Direzione, invia il contributo ad uno o più esperti del tema trattato, designati preferibilmente fra i componenti del Comitato di Valutazione.
Il revisore (o i revisori) formulerà (o formuleranno) il proprio giudizio, tenendo conto dei seguenti parametri:
– correttezza e coerenza dell'impostazione metodologica;
– originalità dello scritto;
– adeguatezza della bibliografia e della giurisprudenza citate;
– chiarezza espositiva.
Sulla base di tali parametri, l'esito del referaggio può comportare: un giudizio di idoneità alla pubblicazione senza modifiche; un giudizio di idoneità alla pubblicazione, subordinato al previo apporto di modifiche e/o integrazioni (che verranno indicate all'Autore); un giudizio di non idoneità alla pubblicazione.
In caso di giudizio discordante fra più revisori, la decisione finale verrà assunta dal Direttore.
In caso di contributi provenienti da Autori di particolare fama o prestigio, il Direttore, sotto la sua responsabilità, può decidere di pubblicare il contributo, senza sottoporlo alla procedura di referaggio.

Volume pubblicato con il contributo finanziario del Dipartimento di Giurisprudenza dell'Università degli Studi di Roma Tor Vergata.
Risultato della ricerca triennale (2021-2023): "Cripto arte: inquadramento giuridico e problemi di circolazione nell'ordinamento interno e internazionale".

L'Archivio della Casa Editrice Cacucci, con decreto prot. n. 953 del 30.3.2022 della Soprintendenza Archivistica e Bibliografica della Puglia-MiC, è stato dichiarato ***di interesse storico particolarmente importante*** *ai sensi degli articoli 10 c. 3, 13, 14 del d. lgs. 42/2004.*

Via Nicolai, 39 – 70122 Bari – Tel. 080/5214220
http://www.cacucciditore.it e-mail: info@cacucci.it

Indice

Il "furto" del non fungible token

Stefano Preziosi*

Sommario: 1. Caratteri generali. – 2. Le fattispecie penali. – 3. Il "furto" di NFT.

1. *Caratteri generali*

Allo stato, per quanto consta, non esistono precedenti giurisprudenziali né elaborazioni teoriche approfondite, nell'ambito dell'ordinamento italiano, sul c.d. furto di *non-fungible token*. La domanda è se questo tipo di *prodotto digitale*, con le sue caratteristiche tecnologiche e giuridiche, ampiamente studiate in altri ambiti del diritto, presenti profili tali da richiederne uno specifico inquadramento in sede penale e, eventualmente, a quale (o quali) fattispecie debba essere riportato, al di là della atecnica classificazione come "furto". Preliminarmente, solo per completezza espositiva, è bene metterne in rilievo alcune peculiarità che sono state già rilevate nell'ambito di approfondimenti non penalistici.

Senza entrare assolutamente nel merito di distinzioni e di sotto tipologie all'interno della categoria dei NFT – aspetti che esulano dalle competenze e dalle finalità di questo scritto – se ne deve sottolineare la caratteristica essenziale e la funzione economico sociale che sembra conferirgli a buon diritto una sostanziale autonomia rispetto ad altri prodotti digitali.

Quanto alla sua caratteristica essenziale, si tratta della *infungibilità*, che consiste nel possedere un attributo specifico non sostituibile con un altro della stessa specie; riguardo alla sua funzione economico sociale, essa è data dall'essere un *asset* unico, che produce contenuti unici «in

* Professore ordinario di Diritto penale presso l'Università degli studi di Roma Tor Vergata.

un ecosistema come quello digitale che è strutturalmente predisposto per replicare gratuitamente in modo illimitato i contenuti senza che le ulteriori copie soffrano alcun degrado in termini qualitativi»,[1] con ciò realizzando la «possibilità di rendere esclusivo l'accesso al contenuto digitale»[2] e, soprattutto, la «creazione artificiale della scarsità come presupposto del valore».[3] A differenza che nei beni fisici e più in generale naturali, pertanto, attraverso tale *strumento* è possibile *creare* scarsità e, conseguentemente, esclusività della fruizione. La scarsità, riguardo ai beni naturali (uso qui l'aggettivo *naturale*, che può comprendere beni fisici ma anche non fisici – quali, ad esempio, una rappresentazione scenica, una lezione, un intervento chirurgico – come oppositivo di *digitale*), è legata ad un bisogno, che la precede come termine di un rapporto economico, ove il *prius* è dato dalla soddisfazione del bisogno ad opera della risorsa scarsa. La risorsa, in natura, appare come termine meramente passivo di questo rapporto, una sorta di nutrimento dell'appetito umano, materiale o morale che sia: il bene/risorsa asseconda il bisogno che ha priorità fenomenologica rispetto al primo. Mediante il prodotto digitale in questione, invece, i termini della suddetta relazione appaiono rovesciati, poiché lo strumento crea scarsità e perfino unicità della risorsa, di guisa che, anzi, il bene finale sembra divenire non la risorsa in quanto tale (il contenuto digitale), ma, piuttosto, la sua unicità, che prende "corpo" – quasi materializzandosi, verrebbe da dire – nel certificato di autenticità autografato, tanto da costituire quest'ultimo, si è detto, il sinallagma contrattuale che sta alla base della sua circolazione/vendita, e non il bene digitale che ne rappresenta il contenuto.[4]

Le caratteristiche dei NFT sono la unicità, indivisibilità e infungibilità. Inoltre, essi circolano all'interno di sistemi di *blockchain*, che garantiscono la provenienza dell'opera, potremmo dire la sua genuinità

---

1 Nava, *I* non-fungible token, in Aa.Vv. *Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia*, a cura di R. Giordano, A. Panzarola, A. Police, S. Preziosi, M. Proto, Milano, 2022, p. 244.

2 *Op. Cit.*, p. 246.

3 *Op. Cit.*, 262.

4 *Op. loc. ult. cit.*

e originalità, ossia la garanzia della corrispondenza fra artista (identità dell'artista, relativamente alle opere d'arte, naturalmente, anche se NFT possono esistere ed esistono in molti altri campi, dallo sport fino alla finanza) e soggetto che, all'interno di tale sistema, vende il NFT (o, eventualmente, soggetto terzo titolare del diritto o avente causa dal titolare).

L'opera NFT nasce e vive su blockchain e risulta intrinsecamente connessa a tutti i dati relativi ai suoi trasferimenti che in quella stessa blockchain sono contenuti e che divengono, quindi, indissolubilmente legati al bene stesso, come se sul NFT fosse stato inciso il nome del proprietario e di tutti i proprietari precedenti. Pertanto, ogni NFT risulta completamente tracciabile e ne viene garantita al massimo grado la titolarità dell'*asset* medesimo. Generalmente la sua esistenza giuridica è collegata ad uno *smart contract*, che oltre a determinarne il contenuto ne consente il suo inserimento all'interno di un sistema di *blockchain* e, quindi, la sua circolazione e utilizzazione.

Come è noto, la *blockchain* è un sistema decentrato di rete, che cioè non fa capo ad un singolo gestore e che si basa su nodi crittografati. Vi possono essere opere native NFT o non native, ossia che hanno un'esistenza meramente digitale o che costituiscono la riproduzione o elaborazione digitale di una realtà fisica. Il loro "valore" può essere legato in parte alla produzione o alla riproduzione digitale e, quindi, alla tecnica e all'originalità di questa, oppure al valore derivante dal diritto di sfruttamento economico sopra un bene qualsiasi o dal diritto di accedere ad una *community*, cui il NFT conferisce valore aggiunto.

2. *Le fattispecie penali*

Dunque, quali comportamenti potrebbero venire in considerazione in chiave di rilevanza penale?

Orbene, circoscrivendo necessariamente la casistica che può astrattamente assumere rilievo, possiamo prendere spunto da alcune vicende che hanno avuto una certa eco mediatica, oltre che un notevole impatto sociale ed economico.

Così, ad esempio, il primo "furto" – così definito dai *mass media* – di NFT avvenuto su OpenSea, uno dei più grandi e famosi negozi di opere digitali. Decine di suoi utenti sarebbero stati vittime di un furto di opere digitali dai loro account, per un valore totale di circa 1,6 milioni di dollari.[5]

Le modalità di realizzazione, sempre stando a quanto riportato dalla stampa e dai canali di comunicazione di Internet, sarebbero consistite nell'aver sfruttato, gli autori dell'illecito, l'occasione di un aggiornamento del protocollo di scambio della piattaforma di blockchain, inviando una mail a molti iscritti con cui si invitava ad effettuare una procedura di *upgrade* del proprio profilo cliccando su un link inserito nel testo. Poi, attraverso uno script venivano sottratte le opere digitali ai "proprietari":[6] opere presumibilmente messe in vendita, successivamente, sul mercato nero.

Si tratta di operazione riconducibile, verosimilmente, al c.d. *phishing*, che, tuttavia, merita qualche riflessione di ordine tecnico giuridico.

Con questo termine si intendono le condotte con cui, mediante artifici o raggiri, si ottengono le credenziali di autenticazione necessarie ad accedere abusivamente a spazi informatici esclusivi del titolare (ad

---

5 Trapani, *Non basta saper comprare NFT per evitare di essere truffati*, *IL FOGLIO*, 23 febbraio 2022.

6 «Un **attacco hacker di phishing** ha sottratto ben **1,7 milioni di dollari in NFT da OpenSea**, uno dei principali mercati online per vendere non-fungible tokens. Gli hacker avrebbero attaccato sabato, ma già domenica i gestori del marketplace hanno assicurato gli utenti che era sicuro produrre, comprare e vendere token sfruttando la blockchain del sito. Le indagini però continuano: **32 le vittime e 254 token trasferiti senza pagamento**…L'attacco è avvenuto durante la migrazione di OpenSea ai sistemi di smart contract di **Wyvern**, iniziata venerdì e che dovrebbe terminare entro il 25 febbraio. Anche se OpenSea **esclude un collegamento** fra l'attacco e la migrazione. Secondo Finzer, l'origine dell'attacco non sarebbe il sito di OpenSea. Infatti ha specificato che **nessuna delle vittime avrebbe cliccato su link sospetti nelle email** che avrebbero sfruttato una vulnerabilità del sito», *OpenSea: rubati 1,7 milioni di dollari in NFT con un attacco hacker***,** in https://*tech**princes.it***, 22 febbraio 2022.

esempio relativi alla gestione dei conti correnti on line) e a svolgere, senza autorizzazione, operazioni bancarie o finanziarie. Condotte che possono dar luogo ai delitti di cui agli art. 494 (sostituzione di persona), 615 ter (accesso abusivo a sistemi informatici o telematici) e 640 *ter* c.p. (Frode informatica). In tal senso viene in considerazione l'uso fraudolento delle credenziali di autenticazione da parte di soggetto diverso da quello autorizzato, che può rilevare in chiave di offesa alla fede pubblica, ai sensi dell'art. 494, cit.; di lesione del bene giuridico del domicilio informatico, *ex* art. 615 *ter*, cit.; di lesione dell'interesse patrimoniale tutelato dal delitto di frode informatica, quale ipotesi speciale di truffa, a termini dell'art. 640 *ter*, cit.

La *frode informatica* introdotta con l. n. 547 del 23 dicembre 1993, è solo apparentemente strutturalmente similare alla truffa di cui all'art. 640, c.p.,[7] poiché, in realtà, non vi figurano gli artifizi e i raggiri, costituenti modalità della condotta tipica di quest'ultima fattispecie. Le condotte tipiche sono infatti rappresentate dall'alterazione (*in qualsiasi modo*, e non da modalità *vincolate* quali sono gli *artifizi* e i *raggiri* che connotano la truffa) di un sistema informatico o telematico (c.d. alterazione esterna del sistema), ovvero dall'intervento senza diritto (con qualsiasi modalità) su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti: «Mentre la prima categoria di condotte descrive interventi in grado di modificare le modalità operative dei sistemi informatici o telematici, attraverso quella che è stata definita un'alterazione "estrinseca", che si attua mediante modifiche delle componenti hardware o software del sistema, la seconda si realizza alterando gli esiti delle attività di elaborazione dei dati, attraverso disparate modalità di accesso e fruizione dei sistemi (e, dunque, rappresentando una classica ipotesi di condotta a forma libera) caratterizzate tutte dall'esser eseguite in difetto delle necessarie autorizzazioni per intervenire e interagire con il sistema: si è così ravvisata l'ipotesi dell'intervento senza diritto su dati e informazioni contenuti in un si-

---

7 Minicucci, *Le frodi informatiche*, in AA.VV. *Cybercrime*, a cura di A. Cadoppi, S. Canestrari, A. Manna, M. Papa, Torino, Milano, 2019, p. 830.

stema informatico sia nelle fattispecie in cui il soggetto, pur legittimato all'acceso al sistema, operi in modo da far risultare alterati i dati e le informazioni procurando un profitto anche ad un terzo, sia nelle situazioni in cui il soggetto agente, senza possedere le credenziali per l'accesso ad un sistema, riesca comunque ad inserirsi abusivamente nel sistema realizzando profitti ingiusti, ad esempio mediante abusivo accesso ad un sistema informatico bancario ed esecuzione di illecite operazioni di trasferimento fondi».[8]

Con riguardo alla problematica qui esaminata sembra venire in inconsiderazione la seconda modalità di condotta, ossia l'intervento senza diritto, abusivo. Nondimeno sembra potersi ipotizzare anche l'altra modalità, ossia la manipolazione del *software*, ove ne sia determinata una anomalia del funzionamento tale da generare una compromissione dei risultati prodotti.[9] Così, nel caso sopra riportato, ad esempio, del furto di NFT avvenuto su OpenSea, la condotta criminosa sarebbe consistita – a quanto pare – nell'aver inviato delle mail agli utenti di quella piattaforma, con cui venivano indotte le vittime ad effettuare un *upgrade* del proprio profilo e, una volta "sottrattogli" questo, nell'avere, mediante un dispositivo informatico (*script*), operato i trasferimenti dei token con le relative opere digitali. Probabilmente, salvo naturalmente un necessario approfondimento tecnico-informatico, la sovrascrittura con gli *script* sembra integrare una alterazione funzionale del sistema; in ogni caso non v'è dubbio che essa configuri un *intervento senza diritto* sui dati e, quindi, condotta tipica del reato *de quo*.

Si possono a questo punto individuare delle peculiarità del "furto" di NFT.

Innanzitutto, ci troviamo di fronte a condotte di *induzione in errore* che, se non sono necessarie quali elementi costitutivi della frode informatica – come già si è detto – sono però elementi costitutivi della sostituzione di persona (art. 494, cit.): l'invio della mail con l'invito ad

---

8 Cass. Pen., Sez. II, 9.2.2023, n. 13713.

9 Bisori, *Le frodi informatiche (artt. 640-ter e 640-quinquies; art. 640-quater)*, in *Diritto penale*, Milano, 2022, Tomo terzo, p. 7300.

effettuare l'*upgrade* del proprio profilo cliccando su un link inserito nel testo, rappresenta senz'altro una induzione in errore. Quanto alla sostituzione illegittima della propria all'altrui persona o all'attribuzione a sé o ad altri di un falso nome, o un falso stato, o una falsa qualità a cui la legge attribuisce effetti giuridici, è elemento che sembra pure sussistere in ipotesi di tal fatta.[10]

Relativamente alla frode informatica (art. 640 *ter*, cit.), fermo restando il carattere tipico delle condotte sopra descritte, con riguardo alla necessità che queste abbiano ad oggetto un sistema informatico o telematico si può precisare quanto segue. Per sistema informatico, a termini dell'art. 1 della Convenzione di Budapest sulla criminalità informatica, deve intendersi *qualsiasi apparecchiatura o rete di apparecchiature interconnesse o collegate, una o più delle quali, attraverso l'esecuzione di un programma per elaboratore, compiono l'elaborazione automatica di dati*; mentre, per sistema telematico deve intendersi *qualsiasi rete di comunicazione gestita con tecnologie informatiche*. Pertanto, non v'è dubbio che le condotte di alterazione o di intervento abusivo sopra descritte effettuate anche su un singolo personal computer e, successivamente, su un sistema di *blockchain*, anche sotto questo profilo debbono considerarsi tipiche ai sensi dell'art. 640 *bis*, cit.

La "sottrazione" di NFT può inoltre assumere rilievo anche con riferimento all'accesso abusivo ad un sistema informatico o telematico (art. 615 *ter*, cit.), come già si è anticipato. Valgono, naturalmente, le stesse definizioni di sistema informatico e telematico date per la frode informatica. Circa la condotta tipica di questo reato, poi, ove l'accesso sia fraudolento risultano superate tutte le problematiche interpretative, oggetto di numerose pronunce anche a sezioni unite, poiché in tal caso si tratta di accesso abusivo in senso stretto, ossia effettuato da un soggetto del tutto privo di titolo abilitativo e, quindi, di aggressione dell'*outsider* privo di qualsivoglia legittimazione all'ingresso nel sistema.

Si possono, tuttavia, ipotizzare anche forme diverse di accesso abusivo connesse alla "sottrazione" di NFT, come nelle ipotesi in cui vi sia

---

10 Di Paolo, *Cyber crime. Il Phishing: prospettive di un delitto*, in *Arch. pen.*, 2017, n. 2, p. 2 ss.

abuso del titolo di legittimazione, ad esempio da parte di fiduciario o comunque di altro soggetto in possesso o nella disponibilità a diverso titolo (legittimo) delle credenziali di accesso. In tal caso la giurisprudenza ritiene che possa configurarsi il reato in parola solo quando vi sia un *abuso oggettivo delle credenziali*, qualora non si tratti di pubblici funzionari o di soggetti che rivestano qualifiche di diritto pubblico. La norma, infatti, a scrutinio dei giudici di legittimità punisce non soltanto l'abusiva introduzione nel sistema, ma anche l'abusiva permanenza in esso contro la volontà di chi ha il diritto di escluderlo, di guisa che si rinviene una volontà contraria tacita in caso di perseguimento di una finalità illecita incompatibile con le ragioni per le quali l'autorizzazione è stata concessa.[11] Con un ultimo arresto[12] il supremo organo nomofilattico ha confermato l'interpretazione secondo la quale la condotta punibile per i soggetti privatistici, al di fuori della introduzione nel sistema in totale assenza di titolo, è solo quella dell'abuso oggettivo; mentre, per i soggetti che rivestano una qualifica pubblicistica (pubblico ufficiale o incaricato di pubblico servizio), e relativamente alla sola ipotesi aggravata contemplata dal comma secondo, n. 1, rileva anche l'abuso soggettivo.[13]

3. *Il "furto" di NFT*

È molto importante rilevare che il delitto di frode informatica è stato interpolato dall'art. 9, comma 1, let. a, d.l. 14 agosto 2013, n. 93, convertito in l. 15 ottobre 2013, n. 119, che vi ha aggiunto il comma terzo, il quale prevede una circostanza aggravante ad effetto speciale della frode informatica "se il fatto è commesso con *furto* o indebito utilizzo

---

11 *Ex multis*, Cass. Pen., sez. V, 6.3.2017, n. 14854.

12 Cass. Pen., S.U., 18.5.2017, n. 41210, con nota di Bertolesi, *Accesso abusivo a un sistema informatico: è reato la condotta del pubblico ufficiale commessa con c.d. sviamento di potere*, in *Dir. Pen. Cont.*, 3 ottobre 2017.

13 A. Cappellini, *I delitti contro la riservatezza informatica*, in Aa.Vv. *Diritto Penale*, Tomo terzo, Milano, 2022, p. 6733.

dell'identità digitale in danno di uno o più soggetti".[14] Circostanza che, peraltro, comporta la procedibilità del delitto *de quo* d'ufficio (comma quarto, come modificato dall'art. 9, comma 1, let. b, cit.). Il legislatore ha così introdotto una nozione di "furto" *fraudolento* (estranea, peraltro, al nostro sistema penale) all'interno di una disposizione che si riporta, piuttosto, alla truffa, anche per collocazione topografica.[15] Con la stessa disposizione, poi, ha pure inserito nell'ordinamento penale l'istituto dell'identità digitale, senza però definirne i contorni, salvo quanto si dirà di qui a poco.

Ciò ha comportato che fosse la giurisprudenza a svolgere l'usuale (ancorché improprio) ruolo di supplenza giudiziaria. Così, la Cassazione si è già pronunciata numerose volte sul significato da attribuire in tale contesto alla nozione di *identità digitale*, affermando, con il primo significativo arresto in materia[16], che, sulla base della definizione elaborata ai fini del Codice dell'amministrazione digitale (in special modo art. 1, let.

---

14 Cajani, *La tutela penale dell'identità digitale alla luce delle novità introdotte dal D.L. 14 agosto 2013, n. 93 (convertito con modificazione dalla l. 15 ottobre 2013, n. 119)*, in *Cass. Pen.*, 3, 2014, p. 314 ss.; Crescioli, *La tutela penale dell'identità digitale*, in *Diritto penale contemporaneo*, 5/2018, p. 265 ss.

15 È opportuno a questo riguardo richiamare l'art. 30 *bis*, d. lg. n. 141 del 13.08.2010, il quale definisce il *furto di identità* nei seguenti termini: «Ai fini del presente decreto legislativo per furto d'identita' si intende:
a) l'impersonificazione totale: occultamento totale della propria identita' mediante l'utilizzo indebito di dati relativi all'identita' e al reddito di un altro soggetto. L'impersonificazione puo' 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 identita' 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)». Si tratta di disposizione che, in realtà, non sembra definire alcun *furto* in senso tecnico e che è strumentale alla istituzione di un sistema pubblico di prevenzione delle frodi in materia di contratti di credito ai consumatori (arg. *ex* art. 30 *ter* dello stesso provvedimento legislativo).

16 Sez. II, 20.9.2022, n. 40862.

u-ter, d. lg. 7 marzo 2005, n. 82, c.d. *Codice dell'amministrazione digitale*), non sarebbe ammissibile limitare l'identità digitale alle sole procedure di validazione adottate dalla Pubblica Amministrazione, come SPID, CIE, firma digitale, escludendo le procedure di accesso mediante credenziali a sistemi informatici a gestione privatistica. Ciò in virtù della constatazione empirica (sic!), sostiene la Cassazione, dell'esistenza di diverse tipologie di identità digitale caratterizzate da soglie diversificate di sicurezza a seconda della natura delle attività da compiere nello spazio digitale e della *ratio legis* intesa a rafforzare la fiducia dei cittadini nell'utilizzazione dei servizi on-line e a porre un argine alle frodi realizzate soprattutto nel settore del credito al consumo mediante furto d'identità.

Le conclusioni cui perviene il Giudice di legittimità appaiono tuttavia curiose, poiché, se è vero che il furto di identità nell'utilizzazione di servizi on-line è fenomeno assai allarmante e che effettivamente la *ratio* della norma appare proprio quella di proteggere non tanto la fiducia dei consociati nei sistemi di autenticazione (poiché altrimenti si sarebbe dovuto prevedere un intervento nel quadro dei delitti contro la pubblica fede, e non in quello dei delitti contro il patrimonio) ma il patrimonio degli stessi, gravemente esposto a questo tipo di frodi, è pur vero che i sistemi di autenticazione richiamati *non sono, o non sono tutti, sistemi di identità digitale*, anche perché l'identità digitale, almeno in ambito privato, deve essere creata dall'interessato con un proprio atto volontario, dunque non scaturisce *ipso facto* dall'utilizzazione di procedure di autenticazione per l'accesso a servizi on-line.[17] Pertanto, l'applicazione

[17] Come sempre è utile un richiamo alle radici dei concetti giuridici. Il concetto di identità della persona viene in evidenza in relazione alla identificabilità e unicità dell'individuo, dove il cognome, il nome, lo pseudonimo, i titoli di varia natura, i simboli araldici, assumono il valore di segni distintivi della persona (cfr. De Cupis, *Il diritto all'identità personale*, Milano, 1949) ed in tal guisa l'identità con i suoi segni distintivi diviene oggetto di diritti personali. Seppure in un ambito estremamente differenziato, quale è quello che caratterizza attualmente l'identità digitale, non è possibile, nondimeno, far velo alla natura giuridica essenziale di qualsiasi forma di *identità*, che deve pur sempre ravvisarsi in qualcosa che definisce nell'insieme un individuo, non potendosi qualificare come tale un mero codice di identifi-

dell'aggravante in parola, in mancanza di un "furto" di identità digitale vera e propria, sembra essere il frutto di applicazione analogica *in malam partem*, basata, appunto, sulla *ratio legis* e su di una asserita lacuna normativa (non si dovrebbe dimenticare che in penale, per definizione, non esistono *lacune*, vigendo il principio di tassatività).

Non solo, l'interpretazione della Corte regolatrice appare oltremodo criticabile, poiché, proprio il *Codice dell'amministrazione digitale*, all'art. 1, let. u-quater, richiamato nella pronuncia citata, definisce l'identità digitale come « la rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità fissate nel decreto attuativo dell'articolo 64». Dunque, la nozione proposta dalla Suprema Corte, non è quella di identità digitale, ma quella diversa di *identificazione informatica* recata dallo stesso art. 1, cit., ma al comma u-ter: «la validazione 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 al fine di garantire la sicurezza dell'accesso». La conclusione obbligata, pertanto, è nel senso che, richiedendo l'art. 640 *ter*, comma terzo, ai fini dell'aggravante in parola, il furto o l'indebito utilizzo dell'identità digitale, ed esistendo nel sistema una precisa definizione legale di identità digitale, l'applicazione di tale norma ad ogni furto di credenziali per l'accesso ad un sistema informatico protetto, costituisce un'applicazione analogica della fattispecie circostanziale aggravante. In realtà il legislatore ha utilizzato la locuzione *identità digitale* che designa un elemento normativo di fattispecie e che ha un puntuale riscontro nella disciplina extrapenale dettata dal Codice dell'amministrazione digitale (di rango legislativo) e integrata da altre fonti sublegislative e non si vede perciò come si possa accedere ad una nozione di identità digitale ricavata dal "comunemente inteso" e da un riferimento normativo diverso (*identificazione informatica*).

---

cazione per l'accesso ad un servizio o per compiere atti di disposizione su beni.

Il sistema dell'identità digitale, infatti, è concepito dal legislatore secondo un *modello pubblico per la gestione delle identità digitali*, come si evince chiaramente dall'art. 64, d. lg. n. 82, cit., che prevede un insieme di presidi volti a garantire tutte le parti interconnesse mediante l'identità digitale, a cominciare dalle architetture di rete fino ai soggetti pubblici e privati che previo accreditamento identificano gli utenti per consentire loro il compimento di attività e l'accesso ai servizi in rete. Questo rende evidente che la sommaria equiparazione di qualsiasi sistema di accreditamento mediante codici di accesso all'identità digitale vera e propria, non riflette assolutamente la disciplina vigente in materia. Ed è altrettanto evidente che il furto dell'identità digitale strumentale alla locupletazione fraudolenta del patrimonio della vittima, integra una lesione giuridica ben maggiore rispetto alla stessa frode realizzata con il furto delle mere credenziali di accesso ad un sistema telematico qualsiasi. Ciò non toglie, naturalmente, che il legislatore possa parificare la frode informatica commessa con il furto delle credenziali di autenticazione per l'accesso ad un qualsiasi sistema telematico con quello realizzato mediante il furto dell'identità digitale, ma si tratta, chiaramente, di una opzione che non può essere demandata all'interprete.

Non si comprende, dunque, come si possa accedere ad una nozione di identità digitale atecnica, basata sul "comune sentire", quando il legislatore la definisce in modo preciso e la norma penale utilizza tale nozione quale elemento normativo di fattispecie. Così, ancora la giurisprudenza più recente, secondo la quale «si deve considerare che l'identità digitale è comunemente intesa 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 nella validazione 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 al fine di garantire la sicurezza dell'accesso».[18]

---

18 Cass. pen., Sez. II, 8.9.2023, n. 38027.

In conclusione e più in generale, se di "furto" si può parlare, con tutte le riserve e le precisazioni sopra riportate, è perché effettivamente la sottrazione di NFT sul piano sostanziale non si inquadra integralmente nelle caratteristiche della frode informatica, poiché questa si esaurisce nel procurare un ingiusto profitto con altrui danno come conseguenze della condotta di alterazione o di intervento senza diritto in un sistema informatico o telematico, mentre, con riferimento ai NFT il risultato tipico della condotta criminosa è che il reo consegue stabilmente la disponibilità di un bene (digitale), dotato di autonomia (unicità) e infungibilità. La qual cosa rende questa forma di frode, dal punto di vista giuridico-sociale, senz'altro più vicina alla nozione di furto che a quella di truffa. Ciò dipende dalle caratteristiche tecniche e giuridiche di questo strumento. E difatti, il file che contiene il prodotto digitale non è presente sulla piattaforma di *blockchain*, ma è lo *smart contract* ad essere tracciato sulla piattaforma insieme a chi compra o vende l'opera digitale mediante una registrazione sulla medesima piattaforma. La registrazione sulla *blockchain* non sembra garantire l'identificazione della persona, ma solo la possibilità di collegare l'entità (informatica) che ha la possibilità di dare esecuzione allo *smart contract* con la piattaforma. Questo comporta che il *token* (e il relativo contenuto digitale) non sia assicurato alla piattaforma di *blockchain* e a quei presidi di sicurezza che ne garantiscono la inviolabilità. Con ciò il NFT sembra assumere i contorni di una sorta di *res* digitale suscettibile di sottrazione e di godimento anche *sine titulo.*

Gli autori

Fiammetta Borgia, *Professore associato di Diritto internazionale presso l'Università degli studi di Roma Tor Vergata*

Gianluca Contaldi, *Professore ordinario di Diritto dell'Unione europea presso l'Università degli studi di Macerata*

Giampaolo Frezza, *Professore ordinario di Diritto civile presso l'Università Lumsa di Palermo*

Enrico Gabrielli, *Professore ordinario di Diritto civile presso l'Università degli studi di Roma Tor Vergata*

Edoardo Marcenaro, *Curatore e collezionista d'arte*

Fabrizio Marongiu Buonaiuti, *Professore ordinario di Diritto internazionale presso l'Università degli studi di Macerata*

Stefano Preziosi, *Professore ordinario di Diritto penale presso l'Università degli studi di Roma Tor Vergata*

Vincenzo Ricciuto, *Professore ordinario di Diritto privato presso l'Università degli studi di Roma Tor Vergata*

Benedetta Sirgiovanni, *Professore associato di Diritto privato presso l'Università degli studi di Roma Tor Vergata*

Quaderni della rivista di diritto privato

1. Rosaria Romano (*a cura di*), *Confini e intersezioni della proprietà intellettuale oggi*, 2017.
2. Claudia Confortini, *Garanzia autonoma e interessi usurari*, 2022.
3. Roberto Calvo, *Il negozio giuridico. Saggi*, 2022.
4. Valentina Di Gregorio, *I contratti di "servizi". Contributo allo studio del sotto-tipo*, 2022.
5. Barbara Francone, *La rilevanza dei controlli interni nelle società per azioni: soluzioni organizzative*, 2022.
6. Serenella Sabina Luchena, *Offerta pubblica di acquisto e regime derogatorio*, 2023.
7. Marco Francesco Campagna, *La sintesi. Studio sul linguaggio contrattuale*, 2023.
8. Enrico Gabrielli, *Studi sul concorso dei creditori*, 2023.
9. Francesco Rossi (*a cura di*), *"L'autonomia privata". Gli studi di Enrico Gabrielli*, 2023.
10. Fiammetta Borgia, Benedetta Sirgiovanni (a cura di), *Intelligenza artificiale e diritto: la cripto-arte e la sua circolazione. Un dialogo interdisciplinare*, 2024.