La direttiva UE 2019/713 del 17 aprile 2019 e la tutela penale dell'uso legittimo delle valute virtuali.

A cura di Rosa Maria Vadalà

***1.I reati previsti dalla direttiva. - 2. Le fattispecie nazionali. - 3. In prospettiva* de iure condendo.**

1. La competenza legislativa penale dell'Unione Europea esercitata con la direttiva in esame muove dal duplice obiettivo di contrastare cospicue fonti di entrate della criminalità organizzata e di apprestare contemporaneamente apposita tutela ai consumatori e alle imprese, garantendo il regolare sviluppo del mercato digitale[1].

In linea con un approccio tecnologicamente neutro, si intende tutelare, attraverso misure penali di contrasto alle frodi, l'uso legittimo degli strumenti di pagamento diverso dai contanti, incluse le valute virtuali, definite come "mezzo di scambio digitale".

Completano il sistema sovranazionale apposite forme di assistenza alle vittime di reato e la previsione delle responsabilità anche delle persone giuridiche per i reati previsti dalla direttiva che siano commessi a loro vantaggio sia da soggetti di vertice, sia da soggetti subordinati, in conseguenza dell'omessa vigilanza da parte dei primi.

La descrizione delle condotte da incriminare è operata partendo dall'individuazione del reato principale di "utilizzazione fraudolenta di strumenti di pagamento diversi dai contanti" seguita dai reati ad esso connessi, differenziati in base al carattere materiale o immateriale dello strumento di pagamento.

In particolare, l'art. 3 della direttiva definisce il reato principale di utilizzazione fraudolenta in considerazione della natura illecita dello strumento di pagamento, dipendente o dalla sua provenienza o dal suo stato di contraffazione/falsificazione.

Gli artt. 4 e 5 definiscono i reati connessi all'utilizzazione fraudolenta, includendovi le condotte sia prodromiche di illecita appropriazione/ottenimento e di contraffazione/falsificazione dello strumento di pagamento, sia quelle successive, ma preliminari rispetto all'utilizzazione, del possesso/detenzione e del procurare per sé o per altri lo strumento illecitamente conseguito o falsificato[2].

---

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

[2]Si riporta di seguito il testo integrale rispettivamente dell'art. 4, rubricato *Reati connessi all'utilizzazione fraudolenta di strumenti di pagamento materiali diversi dai contanti*, e dell'art. 5 rubricato *Reati connessi all'utilizzazione fraudolenta di strumenti di pagamento immateriali diversi dai contanti*: 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*

Con riferimento a quest'ultima condotta non appare chiaro se l'espressione "compresi" che segue l'atto di procurare abbia una funzione specificativa o inclusiva, d'individuazione di ulteriori e differenti modalità.

La prima funzione presupporrebbe l'elencazione di condotte omogenee, ma quelle indicate dalla lett. d) dell'art. 4 lo sono solo parzialmente: vi è omogeneità tra le condotte di ricezione, appropriazione e acquisto, ma non tra queste e quelle di trasferimento, importazione, esportazione, vendita, trasporto e distribuzione.

Le prime modalità di cui alla lett. d) presuppongono, infatti, tutte un atto d'incameramento, mentre le seconde si concretizzano in modalità diverse di cessione/messa in circolazione dello strumento di pagamento materiale contraffatto o illecitamente ottenuto.

Per entrambe le categorie di condotta è prevista, inoltre, la finalità della destinazione all'«utilizzazione fraudolenta», la quale, in realtà, nulla aggiunge in termini di pericolosità a comportamenti, quale quelli di cessione/messa in circolazione, già di per sé lesivi del bene tutelato dell'integrità e del corretto sviluppo dell'economia digitale.

Considerazioni analoghe valgono per i reati previsti alla lett. d) dell'art. 5 della direttiva, in ordine ai quali la locuzione "compresi" ha solo una funzione inclusiva- aggiuntiva di condotte di scambio diverse dall'atto di procurare per sé e per altri, con conseguente riproposizione delle distorsioni sopra segnalate.

La predetta finalizzazione all'utilizzazione fraudolenta, che può essere qualificata in termini di dolo specifico[3], appare invece particolarmente utile per i reati di possesso/detenzione previsti dagli artt. 4 e 5 alle rispettive lett. c). Essa evita, da un lato - trattandosi di reati ostativi - che l'anticipazione di tutela sia del tutto priva di profili d'offensività, mentre consente, dall'altro, l'incriminazione di condotte autonomamente punibili a prescindere dalla ricorrenza di un concorso o complicità con l'autore della falsificazione o contraffazione.

---

uno strumento di pagamento materiale diverso dai contanti rubato, contraffatto o falsificato, a fini di utilizzazione fraudolenta"; 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*".

[3] Per la definizione di questa figura e il relativo inquadramento dogmatico e sistematico si rinvia a PICOTTI, *Il dolo specifico. Un'indagine sugli "elementi finalistici" delle fattispecie penali*, Milano, Giuffré, 1993. Specificatamente sulla funzione tipizzante che ha il fine rispetto alla condotta, prima ancora che al profilo soggettivo del reato, p. 501-502.

A conferma della *ratio* sopra delineata si evidenzia che l'art. 8 impone per tutti i reati di cui agli artt. 4 e 5 la punibilità anche a titolo di concorso, favoreggiamento ed istigazione a commetterli, mentre consente la punibilità anche a titolo di tentativo solo per i reati di cui alle lett. a), b) e d), con esclusione espressa, dunque, delle fattispecie di possesso di strumento materiale e di detenzione di strumento immateriale.

In conseguenza della natura immateriale dello strumento di pagamento, alla lett. a) dell'art. 5 è prevista l'incriminazione della condotta di ottenimento, sempre che abbia comportato la commissione di uno dei reati di cui agli artt. 3 e 6 della direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione.

La predetta previsione appare certamente apprezzabile, se si considera che proprio con riguardo alle valute virtuali l'operato penalmente rilevante di terzi può attaccare direttamente la piattaforma digitale che detiene il *wallet* per l'utente, con una stretta connessione fra i "classici" reati informatici e questi nuovi in esame.

A causa della loro natura digitale, la disponibilità delle valute virtuali si realizza attraverso i portafogli elettronici, che sono meri file di dati, che a seconda della tipologia possono essere memorizzati sul desktop del proprio pc o sul proprio *smartphone* o ancora collegati in rete.

Le condotte di apprensione di questi strumenti hanno, pertanto, tecnicamente ad oggetto la chiave crittografica privata, che associata a quella pubblica consente lo scambio di valuta virtuale; ovvero la password e lo username del sito al quale l'utente le ha affidate.

Per la possibilità segnalata di memorizzazione di questi dati su supporti materiali, come una USB od il proprio pc, anche portatile, sarebbe stato utile indicare come ulteriore condotta da incriminare quella di furto, anziché d'indebita appropriazione che, in maniera restrittiva, sembra rimandare al conseguimento della valuta virtuale solo sul presupposto della previa disponibilità delle relative informazioni o del supporto su cui sono memorizzate[4].

Sempre con riferimento alla sottrazione di valute virtuali, particolarmente appropriato è il reato di cui all'art. 6, che descrive la frode connessa a sistemi d'informazione 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*".

[4] In questo senso depone il considerando 15 da cui risulta che "*per appropriazione indebita si dovrebbe intendere la condotta dell'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*".

Nella predetta fattispecie rientrano prassi illecite sorte con riferimento ai servizi *home banking*, come lo stesso phishing[5], che con alcune varianti è realizzabile anche ai fini dell'acquisizione delle valute virtuali.

Accanto al *phishing*, la realtà ha messo in luce diversi meccanismi di truffa in valuta virtuale, che vanno dal semplice "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 - alla creazione o di finte *ICO*, simili apparentemente a quelle di siti realmente esistenti, o di false offerte di valute virtuali note, o ancora di false *app* di portafogli elettronici mediante le quali attuare le c.d. *wallet address scams*.

Condotte di tal fatta, anche in assenza del conseguimento illecito della valuta virtuale, potranno avere rilevanza penale sulla base delle previsioni dell'art. 7 della direttiva, che impone agli Stati di rendere punibili come reato le condotte aventi ad oggetto la realizzazione e diffusione "di *un dispositivo o di uno strumento, di dati informativi 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*".

Previsione analoga è presente anche nella direttiva 2013/40 con riferimento a dispositivi quali un "*programma per computer, destinato o modificato principalmente al fine di commettere uno dei reati di cui agli articoli da 3 a 6*"[6]. Ma quella in esame appare più restrittiva, perché richiede altresì che il dispositivo sia specificatamente adattato al fine di commettere il reato e che la condotta sia posta in essere con l'intenzione di utilizzarlo per la realizzazione del reato.

In questo modo, l'anticipazione della soglia di rilevanza penale viene contenuta attraverso la duplice previsione della idoneità oggettiva del dispositivo ad usi illeciti e della sua destinazione finalistica alla realizzazione di reati in ordine ai quali la condotta incriminata si pone in rapporto di strumentalità[7].

Per quanto riguarda i livelli sanzionatori, sono fissati dall'art. 9, che stabilisce per il reato di utilizzazione fraudolenta e per i reati connessi, previsti alle lett. a) e b) degli artt. 4 e 5, nonché per

[5] 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, e a FLOR, *Phishing e profili penali dell'attività illecita di "intermediazione" del cd. Financial manager*, in *Diritto penale e processo*, 1/2012, p. 55 ss.

[6] Per l'analisi del contenuto di questa previsione della direttiva sull'attacco ai sistemi d'informazione si rimanda a 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. 757-759.

[7] SALVADORI, *op. cit.*, p. 787, secondo cui con queste tecniche di normazione si tipizza "*la proiezione conflittuale della condotta dell'agente nei confronti del contrapposto interesse facente capo al soggetto passivo anche se di per sé indeterminato*".

quello concernente i mezzi per la loro realizzazione di cui all'art.7, una pena detentiva massima non inferiore a 2 anni.
Il limite minimo della misura massima della pena scende invece ad un anno per i reati stabiliti dalle lett. c) e d) degli artt. 4 e 5. Questa scelta sanzionatoria non appare conforme alla diversità tipologica ed offensiva delle condotte contemplate congiuntamente dalle predette lettere, né al trattamento sanzionatorio più grave stabilito per i reati descritti all'art. 7.
Poco equilibrata appare infatti la scelta del legislatore europeo di punire più severamente condotte, quali quelle di ottenimento/messa a disposizione di mezzi per contraffare od ottenere illecitamente gli strumenti di pagamento, che sono antecedenti rispetto alla detenzione/scambio degli strumenti ottenuti mediante i predetti mezzi, a loro volta costituenti condotte prodromiche rispetto all'utilizzazione fraudolenta: all'arretramento progressivo della soglia della rilevanza penale non corrisponde, cioè, una proporzionata risposta edittale.
Il limite minimo della pena massima è ulteriormente aumentato fino a tre anni per la frode connessa ai sistemi di informazione e fino 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.

2. Gli Stati membri sono tenuti a conformarsi alla direttiva 2019/713 entro il 31 maggio 2021; in vista di tale termine, è opportuno interrogarsi sulla presenza o meno nel nostro ordinamento di fattispecie corrispondenti alle vincolanti indicazioni sovranazionali.
In considerazione dell'oggetto dei reati della direttiva, non rilevano ai fini della presente indagine i delitti di falsità o alterazione di monete, contemplati al capo I del titolo VII del libro II del codice penale italiano, i quali sono relativi esclusivamente alla moneta fisica avente corso legale nello Stato o fuori di esso.
A prescindere, infatti, dalla diversità dell'oggetto materiale, che potrebbe essere superata con l'introduzione di una previsione di equivalenza espressa, le fattispecie monetarie di falso, detenzione e spendita di cui agli artt. 453, 454, 455, 457 e 461 c.p. coincidono dal punto di vista modale solo parzialmente con le prescrizioni della direttiva.
In una prospettiva *de iure condito*, la punizione delle condotte indicate dal legislatore europeo potrebbe, di contro, essere attuata attraverso i reati di truffa, ricettazione, indebito utilizzo e falsificazione di carte di credito e di pagamento, nonché mediante i reati informatici previsti dagli artt. 615 *ter*, 615 *quater,* 617 *quinquies* c.p..

Sarebbe, ad esempio, sanzionabile ai sensi dell'art. 640 c.p., quale ottenimento illecito di uno strumento di pagamento immateriale diverso dal contante, la condotta di chi prospettando finti servizi, si faccia dare quale "prezzo" valute virtuali, incamerandole senza alcuna contropartita.

Per punire la frode connessa ai sistemi di informazione, di cui all'art. 6 della direttiva, risulta invece applicabile il delitto di frode informatica.

La fattispecie prevista dall'art. 640 *ter* c.p. è stata introdotta proprio al fine d'incriminare quelle ipotesi in cui l'azione fraudolenta non è indirizzata alla persona che subisce o determina la perdita patrimoniale, ma al funzionamento di un sistema informatico o telematico, che viene alterato o ai dati, alle informazioni e ai programmi in esso contenuto, operando un intervento senza diritto[8].

Il predetto reato, a cui la giurisprudenza fa comunemente ricorso per l'incriminazione del *phishing*, è descritto in maniera assai ampia, richiamando genericamente ogni atto di "procurare per sé o per altri un ingiusto profitto", mentre l'art. 6 della direttiva fa riferimento al più specifico e limitato "atto di effettuare o indurre un trasferimento di denaro, valore monetario o di valuta virtuale".

Anche per quanto riguarda l'oggetto e l'eziologia della condotta, l'art. 6 presenta un contenuto più dettagliato e limitato rispetto a quello previsto dall'art. 640 *ter* c.p., che fa, invece, riferimento alle condotte di "alterazione" in qualsiasi modo del funzionamento di un sistema informatico, certamente inclusiva della condotta di "ostacolo" indicata dalla direttiva, e a quella d'intervento "senza diritto" non solo sui dati, ma anche sulle informazioni e programmi del sistema.

L'utilizzo, con riferimento alle due condotte, dell'espressioni "in qualsiasi modo" e "con qualsiasi modalità" permette di ricomprendere coomportamenti diversi ed ulteriori rispetto a quelli indicati dalla direttiva, consentendo alla fattispecie di restare al passo con l'evoluzione della fantasia dei cybercriminali. Unico aspetto su cui potrebbe essere utile intervenire, per rispettare le prescrizioni della direttiva, riguarda il "declassamento" del profitto ingiusto da evento, qual è oggi previsto dall'art. 640 *ter* c.p., a requisito finalistico soggettivo, che non sia necessario conseguire per la consumazione del reato.

[8] Si rimanda in ordine all'esame dei contenuti di questo delitto a 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; BARTOLI, *La frode informatica tra "modellistica", diritto vigente, diritto vivente e prospettive di riforma*, in *Dir. inf.*, 3/2011, p. 383 ss; PICOTTI, *Reati Informatici*, in *Enc. Giur. Treccani,* Aggiornamento, VIII, Roma, 2000, p. 1 ss.

Nella realtà applicativa frequente è la contestazione, insieme alla frode informatica, dei reati cui agli artt. 615 *ter*[9] e 615 *quater*[10] c.p., rispettivamente di accesso abusivo e di detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici.

Le predette disposizioni rilevano ai fini del presente lavoro nella misura in cui consentono, in assenza d'interventi riformatori appositi, l'incriminazione, con limiti edittali conformi, delle condotte relative ai mezzi per commettere i reati di frode e falsificazione di cui all'art. 7 della direttiva.

Rispetto alle prescrizioni della direttiva le due previsioni appaiono per certi versi meno restrittive e calibrate su esigenze di tutela ulteriori o connesse a quelle relative al mercato unico digitale ed interessanti direttamente la riservatezza informatica, e, in via finale, anche la sicurezza informatica[11].

Stesso discorso può essere svolto con riferimento al delitto di frode informatica, il quale presenta un ambito ontologico certamente più ampio del confine delineato della direttiva in esame.

Depone in questo senso il rigorismo sanzionatorio che connota la fattispecie codicistica, se perpetrata con furto o indebito utilizzo dell'identità digitale[12]. Con la predetta aggravante, che ha destato perplessità e critiche della dottrina[13], il legislatore nazionale esprime sul piano penale quel disvalore che a livello sovranazionale, invece, è considerato [14] solo ai fini della predisposizione di misure di sostegno e protezione per le vittime delle frodi in esame.[15]

---

[9] In ordine ai contenuti di questo delitto si rinvia a FLOR, *Art. 615 ter c.p.: natura e funzioni delle misure di sicurezza, consumazione del reato e bene giuridico protetto*, in *Dir. pen. proc.*, 2008, 106 e ss.; ID., *Sull'accesso abusivo ad un sistema informatico o telematico: il concetto di domicilio informatico e lo jus excludendi alios*, in *Dir. pen. proc.*, 2005, 85 e ss, Cass. pen., Sez. un., 27 ottobre 2011 (dep. 7 febbraio 2012), in Riv. trim. dir. pen. ec., 2012, p. 369, con commento di 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.*

[10] Sulle condotte sanzionate e gli altri elementi costitutivi del delitto in esame si rinvia a SALVADORI, *Criminalità informatica e tecniche di anticipazione della tutela penale. L'incriminazione dei "dual-use software", cit., p. 760-762.*

[11] In questo senso PICOTTI, *Sicurezza, informatica e diritto penale*, in DONINI, PAVARINI (cur.), *Sicurezza e diritto penale*, Bologna 2011, 217 ss.; ID., *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati,* in ID. (a cura di), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004, p. 21 ss.

[12] Sul punto si rinvia a FLOR, *Phishing, identità theft e identità abuse*, in *Riv. It. Dir. e proc. Pen.*, 2007, p. 899 ss.; CRESCIOLI, *La tutela penale dell'identità digitale*, in *Diritto Penale Contemporaneo*, Rivista trimestrale 5/2018.

[13] Si rinvia in proposito a MARGIOCCO, *Frode informatica*, in FINOCCHIARO – DELFINI (a cura di), *Diritto dell'informatica*, Assago, 2014, p. 1107 ss.; MALGIERI, *La nuova fattispecie di "indebito utilizzo d'identità digitale": un problema interpretativo*, in *Diritto Penale Contemporaneo*, Rivista trimestrale, fasc 2/2015, p. 149 ss.

[14] Sul punto si noti la diversità di scelte d'incriminazione operate con l' art. 9, paragrafo 5, della direttiva 2013/40, che, invece, ha prescritto che "*Gli Stati membri adottano le misure necessarie ad assicurare che, qualora i reati di cui agli articoli 4 e 5 siano commessi abusando dei dati personali di un'altra persona allo scopo di guadagnare la fiducia di terzi, in tal modo arrecando un danno al legittimo proprietario dell'identità, ciò possa, conformemente al diritto nazionale, essere considerato una circostanza aggravante, purché tale circostanza non sia già contemplata da un altro reato punibile a norma del diritto nazionale*".

[15] Al Considerando 31, partendo dalla circostanza che "*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*", si auspica che Gli Stati membri possano predisporre misure di aiuto, sostegno e protezione per attenuare tali conseguenze.

Più complessa appare, viceversa, l'incriminazione delle condotte di falsificazione, contraffazione, detenzione-trasferimento degli strumenti di pagamento ottenuti illecitamente o contraffatti.
Ai fini del reperimento delle disposizioni nazionali eventualmente applicabili, utile è la distinzione tra strumenti di pagamento materiali ed immateriali.
Per i primi vengono in rilievo le fattispecie d'indebito utilizzo e falsificazione di carte di credito e di pagamento, nonché di ricettazione, previste dagli artt. 493 *ter* e 648 c.p..
L'art. 493 *ter* c.p., che riproduce in totale continuità la previsione dell'art. 12 del d.l. n. 143/1991, trasfusa poi nel co. 9 dell'art. 55 del d.lgs. 231/2007[16], punisce, in particolare, con la reclusione da uno a cinque anni e con la multa da 310 a 1.550 euro, chiunque, al fine di trarne profitto, indebitamente utilizza, non essendone titolare, falsifica o altera 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 prestazioni di servizi, oppure possiede, cede o acquisisce tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi.
Se per la comune ricettazione la formulazione legislativa sembra rinviare ad una *res* suscettibile di apprensione, il predetto reato "speciale" viene, invece, dalla giurisprudenza unanime applicato anche alle operazioni eseguite mediante utilizzo del numero e dei codici della carta, in assenza della detenzione del supporto materiale del mezzo di pagamento.
Un'interpretazione di questo tipo consente, a formulazione invariata della previsione, d'incriminare anche i reati di detenzione abusiva e falsificazione dei mezzi di pagamento immateriali previsti dalla fonte sovranazionale che, in assenza di profili di frode riconducibili ai reati di cui agli artt. 640 e 640 *ter* c.p., sarebbero prive di risposte sanzionatorie a livello nazionale.
In ordine all'incriminazione delle condotte descritte dalla direttiva rileva, inoltre, il delitto d'installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche, di cui all'art. 617 *quinquies c.p.*[17].
Il predetto reato di pericolo, consistente nell'istallazione di strumenti per la captazione illecita di comunicazioni tra sistemi informatici contenenti ad es. credenziali di accesso personali, si pone in termini strumentali rispetto alla clonazione cui è finalizzata e che, ove realizzata, va ritenuta punibile in progressione criminosa ai sensi dell'art. 493 *ter*.

[16] 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 d codice nella materia penale. Si rinvia per un esame critico di questo delitto quale reato a più fattispecie a GALANTE, *La tutela penale delle carte di pagamento*, in CADOPPI-CANESTRARI (a cura di), *Cybercrime,* collana *Diritto e procedura penale dell'informatica*, utet, 2019, p. 285 ss.
[17] Sulla genesi di questa fattispecie e la sua riformulazione in virtù della legge di ratifica della Convenzione *Cybercrime* del Consiglio d'Europa cfr. PICOTTI, *Profili di diritto penale sostanziale*, in *Dir. pen. proc.*, n. 6/2008, p. 700 ss.

3. Alla luce delle prescrizioni della direttiva e delle fattispecie nazionali applicabili, in prospettiva *de iure condendo* andrebbe valutata l'introduzione di un capo organico ed apposito in materia di falsificazione e frode che riguardi gli strumenti di pagamento diversi dal contante, simile a quello concernente il falso nummario, le cui fattispecie non possono essere semplicemente estese.

Nella stessa prospettiva andrebbe rivisto, anche, il catalogo dei reati presupposto della responsabilità degli enti mediante l'inserimento, come prescritto dalla fonte sovranazionale, nell'elenco del d.lgs. 231/2001 dei delitti di frode informatica e d'indebito utilizzo e falsificazione di carte di credito o di pagamento[18].

Per il resto, le fattispecie italiane esaminate sembrano già rispondenti alle indicazioni europee, risultando per certi versi anche più complete, perché astrattamente applicabili e pensate per una fenomenologia criminale più ampia e complessa[19], che può riguardare, ma non solo, gli strumenti di pagamento diversi dai contanti.

Nonostante tale rilievo, il recepimento della direttiva potrebbe essere l'occasione per una sistemazione organica dei reati informatici intorno a quello che sembra delinearsi come comune bene finale di categoria, ovvero l'"*oggetto di tutela categoriale: l'affidabilità e la sicurezza del ricorso alla tecnologia informatica, telematica e cibernetica*"[20].

Il predetto sostrato assiologico è alla base della esaminata direttiva 2019/731 UE, la quale "*attraverso la punizione di condotte che possono essere realizzate o "manifestarsi" in ambito digitale o nel contesto tecnologico – se non esclusivamente in simili contesti – intende rafforzare il sistema di protezione previsto dalla direttiva relativa agli attacchi contro i sistemi di informazione*"[21].

---

[18] La mancata previsione di questi delitti appare oggi ingiustificata e foriera d'inammissibili vuoti di tutela se confrontata con la previsioni all'art. 24 della frode informatica a danno dello Stato e all'art. 24 bis di altri reati informatici

[19] In proposito PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in ID. (cur.), *Il diritto penale dell'informatica nell'epoca di Internet*, Padova, 2004; ID., *Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale*, in *Dir. Internet*, 2005, 2, 189 e ss., il quale rileva criticamente come la legge 23 dicembre 1993, n. 547, abbia modificato il codice penale con norme inserite nei diversi titoli e seguendo criteri che rendessero i reati informatici il più possibile assimilabili al tessuto preesistente anche sul piano dei beni giuridici tutelati, mediante l'introduzione di nuove modalità di lesione o di diversi oggetti passivi.

[20] 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 di concepire i singoli beni individuali offesi (ad es. patrimonio, riservatezza, proprietà intellettuale) "*come marcatori di zona, per graduare la gravità delle fattispecie*".

[21] Testualmente FLOR, *Cibersecurity 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. 460. L'autore evidenzia come la direttiva in esame, nel "*promuovere un ambiente sicuro, affidabile e più resiliente per i mezzi di scambio digitali*" richiama espressamente la 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*".

La centralità ai fini economici dei predetti sistemi, in particolare nell'odierno pervasivo *cyberspace*, impone di presidiare, anche con risposte penali, il fisiologico sviluppo delle transazioni economiche che avvengono loro tramite e quindi la loro integrità e sicurezza[22].

Le incriminazioni previste dalla direttiva sono orientate a questa logica, richiedendo, a presidio dell'affidabilità del mercato digitale, l'illiceità dell'ottenimento dello strumento di pagamento od il carattere falsificato di questo od ancora l'operare "intenzionalmente" e "senza diritto" [23] con finalizzazione all'utilizzazione fraudolenta.

In questa prospettiva la tutela del patrimonio personale è garantita in virtù e grazie alla tutela della sicurezza informatica cibernetica, che, in forza della pervasività della rete, è elevata ad "*interesse primario e per certi aspetti totalizzante, non solo della persona, ma anche o prima di tutto della collettività*"[24].

[22] Cfr. 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*, *cit*., p. 70; ID., *Cybersecurity: quid novi?*, in *Diritto di Internet*, n. 1/2020, p. 11, che 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*".

[23]Sulle implicazioni di diritto penale sostanziale derivanti dalla previsione in tutte le fattispecie considerate dalla Convenzione Cybercrime, promossa dal Consiglio d'Europa ed approvata a Budapest il 23 novembre 2001, della commissione, sul piano oggettivo, "senza diritto" e su quello soggettivo "intenzionalmente" v. PICOTTI, *Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale*, *cit*., p. 197-198.

[24] Testualmente PICOTTI, *op. cit*., p. 12, l'Autore rileva, espressamente, a p. 13 come "*oggi la "sicurezza cibernetica" (cybersecurity) ha assunto un'importanza ed una dimensione ancor più ampie e pervasive, che si manifestano in un approccio anche giuridico radicalmente diverso. Si deve infatti muovere dal riconoscimento che dalle reti e dai sistemi informatici dipendono ormai funzioni e servizi essenziali, per la società, l'economia, i diritti e gli interessi pubblici e privati. L'approccio è quindi quello di assicurare, a livello generale, un elevato grado di sicurezza delle reti e dei sistemi in quanto tali, avendo essi stessi acquisito il rango di autonomi "beni giuridici""*.