ATTUALITÀ

CHIARA CRESCIOLI

Le recenti modifiche ai reati cibernetici, tra tardivo recepimento delle direttive europee e nuove incriminazioni: riflessioni critiche

Il presente contributo analizza i due provvedimenti legislativi nazionali di attuazione della direttiva 2019/713/UE relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti e della direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione. In particolare, l'analisi si concentra sull'esame delle modifiche apportate alla fattispecie di indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti e ai reati contro la riservatezza informatica, nonchè sulle criticità irrisolte.

Critical considerations about recent legal reforms for tackling cybercrime between late transposition of European Directives and new criminal offences

This paper analyses the transposition of Directive (EU) 2019/713 on combating fraud and counterfeiting of non-cash means of payment and Directive (EU) 2013/40 on attacks against information systems in Italian legislation. The analysis will focus on the amendments made to the offences of misuse or falsification of payment instruments and illegal system interference, illegal data interference and illegal interception and the remaining critical issues.

1. *Introduzione.* Nell'arco di poco più di un mese, il legislatore italiano ha approvato due diversi provvedimenti che hanno inciso in modo significativo sul diritto penale dell'informatica. Si tratta del d.lgs. 8 novembre 2021 n. 184, di attuazione della direttiva 2019/713/UE relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti, e della L. 23 dicembre 2021, n. 238, vale a dire la legge per l'adempimento degli obblighi deri-

vanti dall'appartenenza dell'Italia all'Unione europea (c.d. legge europea 2019-2020).
Con la direttiva 2019/713/UE il legislatore europeo ha previsto diversi obblighi di incriminazione concernenti le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti, al fine di armonizzare le diverse legislazioni penali degli Stati membri tramite l'adozione di misure di diritto penale, in grado di contrastare un grave fenomeno transfrontaliero che costituisce una seria minaccia per l'efficacia del mercato unico europeo.
La direttiva 2013/40/UE, a cui l'art. 19 della L. 23 dicembre 2021, n. 238 è volto a dare piena attuazione, è relativa, di contro, agli attacchi contro i sistemi di informazione e prevede diversi obblighi di incriminazione allo scopo di garantire il buon funzionamento e la sicurezza dei sistemi di informazione, fondamentali per lo sviluppo del mercato unico europeo, tramite l'armonizzazione delle legislazioni penali sostanziali.
Nel prosieguo verranno esaminati soltanto gli atti interni di recepimento della direttiva 2013/40/UE e direttiva 2019/713/UE, i quali, seppur caratterizzati da note positive, presentano alcune lacune e, sul piano della formulazione delle norme incriminatrici, talune anomalie che non consentono di ritenere pienamente attuati gli obblighi di incriminazione previsti dal legislatore europeo.

2. *L'attuazione della direttiva 2019/713/UE relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti.* Il d.lgs. 8 novembre 2021 n. 184, di attuazione della direttiva 2019/713/UE dedicata alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti, è entrato in vigore il 14 dicembre 2021. L'obiettivo perseguito dal legislatore europeo attraverso questa direttiva, che ha sostituito la decisione quadro 2001/413/GAI, consiste nell'adottare misure di diritto penale efficaci ed efficienti al fine di proteggere i mezzi di pagamento diversi dai contanti da frodi e falsificazioni[1]. Si è, infatti, osservato che le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti non solo costituiscono una minaccia per la sicurezza, dato che il denaro illecitamente sottratto alle vittime spesso viene impiegato per finanziare la criminalità organizzata, ma minano lo sviluppo del

[1] V. il *Considerando* n. 13 della direttiva 2019/713/UE.

mercato unico digitale, poiché inducono i cittadini a diffidare dei nuovi strumenti digitali di pagamento. Tale diffidenza nel nostro Paese è più elevata che nel resto d'Europa[2].
Il legislatore europeo ha scelto di intervenire in tale ambito prevedendo sia obblighi di incriminazione, sia obblighi relativi allo scambio di informazioni e comunicazione dei reati, all'assistenza e al sostegno alle vittime e alla prevenzione. Per adeguare la normativa interna alla direttiva sopra indicata, il decreto di attuazione è intervenuto sul codice penale, sul d.lgs. 8 giugno 2001, n. 231 in materia di responsabilità da reato delle persone giuridiche e, infine, ha introdotto ulteriori disposizioni normative al fine di assicurare la trasmissione di dati e informazioni.

3.1. *Le modifiche alla fattispecie di indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti cui all'art. 493-*ter *c.p.* Il d.lgs. 184 del 2021 ha modificato l'art. 493-*ter* c.p., ora rubricato «*indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti*», ampliando l'oggetto del reato sino a ricomprendere tutti gli strumenti di pagamento diversi dai contanti, oltre alle carte di credito. Infatti, la precedente fattispecie già prevista era imperniata sul concetto di "documento", che richiedeva una sua fisicità. Tale modifica legislativa ha adeguato la fattispecie ai mutamenti tecnologici, dato che in precedenza l'oggetto di tutela era necessariamente un documento, per cui era dibattuto se la tutela apprestata dalla norma potesse essere estesa anche ai dati identificativi delle carte di credito o pagamento[3].
Grazie all'ampia formulazione adottata tramite l'inserimento del sintagma espansivo «*o comunque ogni altro strumento di pagamento diverso dai contanti*», questo problema può oggi dirsi superato. Infatti, tale assunto è indice del passaggio dalla tutela della carta di credito in senso materiale, alla tutela

[2] Nell'indice europeo relativo al *Digital Market and Society* viene stabilito che «*Denmark, Finland, Sweden and the Netherlands have the most advanced digital economies in the EU followed by Luxembourg, Belgium, the UK and Ireland. Romania, Bulgaria, Greece and Italy have the lowest scores on the DESI*», disponibile *online* al sito https://ec.europa.eu/digital-single-market/en/desi.
[3] GALANTE, *La tutela penale delle carte di pagamento*, in *Cybercrime*, a cura di Cadoppi-Canestrari-Manna-Papa, Torino, 2019, 289.

delle funzioni di pagamento cui il supporto abilita, ora svolte, ad esempio, anche da uno *smartphone* o da uno *smartwatch.*

Il legislatore italiano all'art. 1 d.lgs. cit. ha poi fornito le definizioni di «strumento di pagamento diverso dai contanti», «dispositivo, oggetto o record protetto», «mezzo di scambio digitale» e «valuta virtuale»[4]. Tali definizioni sono identiche a quelle contenute nella direttiva e inserite dal legislatore europeo proprio al fine di garantire uniformità nella sua applicazione, facilitando la cooperazione tra le autorità competenti.

La definizione di «strumento di pagamento» specifica che esso può essere immateriale o materiale. Si può, dunque, affermare, senza ombra di dubbio, che oggetto del reato di cui all'art. 493-*ter* c.p. siano anche le *App* per *smartphone* e i programmi *software* di *home banking* diffusi dalle Banche per effettuare pagamenti *online*. Poiché non è specificato che lo strumento in questione debba essere necessariamente controllato da una banca centrale o da un ente pubblico, si ritiene che oggetto di tutela siano anche piattaforme di *mobile payment*, quale ad esempio *satispay* o *PayPal*, che consentono di inviare a e ricevere fondi da altri utenti della stessa *App* senza utilizzare i circuiti di carte di credito e debito tradizionali. Per il resto l'art. 493-*ter* c.p. è rimasto invariato, perché si tratta sempre di una disposizione a più norme, che prevede tre fattispecie delittuose: l'"indebito utilizzo", la "falsificazione" o l'"alterazione" e, infine, il "possesso", la "cessione" o l'"acquisizione" degli strumenti di pagamento indicati di provenienza illecita[5].

L'ampliamento dell'oggetto "materiale" del reato di cui all'art. 493-*ter* c.p. pone qualche difficoltà di coordinamento con la fattispecie di frode informatica. Infatti, in materia di utilizzo carte di credito clonate era già sorto un contrasto giurisprudenziale circa la qualificazione giuridica del fatto[6]. Secondo un

---

[4] Con riferimento alla definizione di "valuta virtuale" si condividono le riflessioni di PICOTTI, *«Nuovi» crimini cibernetici e possibile rilevanza penale dell'intelligenza artificiale. Atti digitali del convegno gli Stati Generali del diritto di Internet, Luiss, 16,17,18 dicembre 2021*, in *Diritto di Internet*, 2022, supplemento 1, 11, che sottolinea l'inadeguatezza della validità di tale definizione "ai soli effetti della legge penale", dato che le valute virtuali rientrano in un complesso ben più ampio di regolamentazioni extrapenali.

[5] BERTOLESI, *Sub art. 493*-ter, in *Codice penale commentato*[5], a cura di Dolcini-Gatta, Milano, 2021, § 6; CORRADINO, *La tutela penale del sistema dei pagamenti nell'abuso di carta di credito*, in *Banca, borsa, tit. cred.*, 2001, 1, 121.

[6] Contrasto giurisprudenziale rilevato anche da Cass., Sez. II, 14 febbraio 2017, n. 8913, la quale tuttavia

primo orientamento, la fattispecie applicabile sarebbe unicamente la frode informatica, in quanto l'elemento specializzante consisterebbe nell'utilizzazione "fraudolenta" del sistema informatico, che assorbirebbe la generica indebita utilizzazione di una carta di credito[7]. Per un diverso orientamento, invece, esso integrerebbe il reato di indebita utilizzazione di carte di credito e non quello di frode informatica il prelievo di denaro contante presso lo sportello *bancomat* di una banca mediante l'abusivo utilizzo di supporti magnetici con dati clonati, perché non vi sarebbe né l'alterazione del sistema informatico o telematico, né l'abusivo intervento sui dati, ovvero non sarebbe integrato il fatto tipico della frode informatica[8].

Il quadro normativo è stato ulteriormente complicato, perché se prima della modifica legislativa si riteneva che l'uso di codici e numeri di carte di credito clonate per penetrare abusivamente nel sistema informatico bancario ed effettuare indebitamente operazioni integrasse la sola fattispecie di frode informatica e non l'indebita utilizzazione di carte di credito[9], ora non è più così pacifico. Infatti, in precedenza si riteneva che l'elemento specializzante dell'utilizzazione "fraudolenta" del sistema informatico, dunque la sua alterazione, costituisse presupposto "assorbente" rispetto alla generica indebita utilizzazione dei codici d'accesso. Tuttavia, gli strumenti di pagamento diversi dai contanti non possono essere falsificati se non attraverso l'alterazione di dati o programmi informatici o comunque il loro indebito utilizzo, dato che si tratta di strumenti immateriali. L'elemento dell'alterazione, dunque, perde il suo carattere di specialità e diventa difficile individuare quale sia la norma prevalente.

---

non si è pronunciata sul punto, limitandosi ad annullare senza rinvio la sentenza impugnata per intervenuta prescrizione.

[7] In tal senso Cass., Sez. II, 15 aprile 2011, n. 17748, secondo cui «*integra il delitto di frode informatica, e non quello di indebita utilizzazione di carte di credito, colui che, servendosi di una carta di credito falsificata e di un codice di accesso fraudolentemente captato in precedenza, penetri abusivamente nel sistema informatico bancario ed effettui illecite operazioni di trasferimento fondi, tra cui quella di prelievo di contanti attraverso i servizi di cassa continua*»; in senso conforme anche Cass., Sez. II, 13 ottobre 2015, n. 50140, la quale in motivazione ritiene decisiva la sussistenza dell'elemento specializzante, costituito dall'utilizzo "fraudolento" del sistema informatico. Per la dottrina v. LAZZARI, *Riciclaggio di carte di credito e truffa: concorso di reati o concorso di norme?*, in *Cass. pen.*, 2001, 9, 2473.

[8] Così Cass., Sez. VI, 14 gennaio 2016, n. 1333.

[9] V. Cass., Sez. II, 21 luglio 2020, n. 21831; Cass., Sez. II, 9 maggio 2017, n. 26229; Cass., Sez. II, 13 ottobre 2015, n. 50140; Cass., Sez. II, 15 aprile 2011, n. 17748.

I primi commentatori hanno proposto di ritenere applicabile l'art. 493-ter c.p. a tutte le ipotesi di utilizzo illegittimo di mezzi di pagamento immateriali e di considerare come residuale l'art. 640-*ter* c.p., nell'ipotesi aggravata di nuova introduzione[10]. Tuttavia, tale soluzione non è condivisibile, perché finirebbe per abrogare tacitamente e limitare eccessivamente l'applicabilità della frode informatica. Infatti, per la stessa struttura della fattispecie, che richiede l'alterazione o l'intervento senza diritto su un sistema informatico, la commissione di frodi informatiche attraverso strumenti che non siano proprio quelli di pagamento diversi dai contanti appare residuale, mentre soltanto la fattispecie di frode informatica prevede la circostanza aggravante del fatto commesso con furto o indebito utilizzo dell'identità digitale. La frode informatica, ai fini della sua integrazione, richiede però l'effettivo conseguimento di un ingiusto profitto con altrui danno, per cui nell'ipotesi di clonazione e successivo indebito uso di uno strumento di pagamento si potrebbe ritenere che la frode informatica aggravata sia idonea a sanzionare il fatto considerato nel suo intero disvalore, ricomprendendo sia la falsificazione o l'alterazione, sia il successivo utilizzo con sottrazione indebita del denaro altrui[11]. Inoltre, dato che il reo sfrutta le credenziali della vittima fingendosi quest'ultima per effettuare operazioni non autorizzate, tale condotta può essere ricompresa nella nozione di «*indebito utilizzo dell'identità digitale*» di cui al co. 3 dell'art. 640-*ter* c.p. Per questo motivo, si può ritenere che nei casi in cui si sia verificato l'effettivo depauperamento della vittima, l'indebito utilizzo, la falsificazione o l'alterazione dello strumento di pagamento possano considerarsi assorbite nel più grave reato di frode informatica aggravata di cui all'art. 640-*ter* co. 2 e 3 c.p.

3.2. *L'introduzione del nuovo reato di detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti fattispecie di cui all'art.*

[10] In tal senso v. BERNARDONI, *Attuazione degli obblighi europei in materia di lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti: prima lettura del d.lgs. n. 184 del 2021*, in *www.sistemapenale.it*, 3 febbraio 2021.

[11] In tal senso anche PICOTTI, *Sistematica dei reati informatici, tecniche di formulazione legislativa e beni giuridici tutelati*, in *Il diritto penale dell'informatica nell'epoca di Internet*, ID., Padova, 2004, 57.

493-quater *c.p.* All'art. 493-*quater* c.p. è stato introdotto il nuovo delitto di «*detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti*», che sanziona chiunque, al fine di farne uso o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti, produce, importa, esporta, vende, trasporta, distribuisce, mette a disposizione o in qualsiasi modo procura a sé o ad altri apparecchiature, dispositivi o programmi informatici che, per caratteristiche tecnico-costruttive o di progettazione, sono costruiti principalmente per commettere tali reati, o sono specificamente adattati al medesimo scopo. Vi è, quindi, una discrasia tra la rubrica della norma e le condotte sanzionate. Infatti, la mera detenzione di apparecchiature, dispositivi e programmi non è indicata nel testo tra le condotte punite, ma lo sono soltanto la produzione o la messa a disposizione, alle quali non può essere assimilato il mero possesso[12], e il procurarsi. Trattasi, dunque, sulla falsariga dell'art. 615-*quater* c.p., di reato di pericolo indiretto che sanziona condotte prodromiche alla commissione di ulteriori illeciti relativi agli strumenti di pagamento diversi dai contanti. Il parallelismo con quest'ultima fattispecie è evidente: anche in questo caso la tutela penale viene anticipata e l'elemento soggettivo previsto è il dolo specifico, che in questo caso svolge una fondamentale e peculiare funzione "tipizzante", trattandosi di condotte c.d. neutre[13]. In particolare, l'art. 494-*quater* c.p. prevede che il reo debba agire «*al fine di farne uso o di consentirne ad altri l'uso nella commissione di reati riguardanti strumenti di pagamento diversi dai contanti*».

Una differenza significativa risiede nel fatto che, a differenza dell'art. 615-*quater* c.p.[14], nel nuovo art. 493-*quater* c.p. è stata espressamente inserita la clausola di sussidiarietà «*salvo che il fatto costituisca più grave reato*», renden-

[12] V. SALVADORI, *I reati contro la riservatezza informatica*, in *Cybercrime*, a cura di Cadoppi-Canestrari-Manna-Papa, Torino, 2019, 694, che evidenzia come il "procurarsi" concerna attività che precedono logicamente la detenzione.

[13] Sulla struttura e sul ruolo del dolo specifico v. PICOTTI, *Il dolo specifico. Un'indagine sugli "elementi finalistici" delle fattispecie penali*, Milano, 1993, 471 ss.

[14] In mancanza di clausola di sussidiarietà espressa, i rapporti tra gli artt. 615-*ter* e 615-*quater* c.p. sono tuttora controversi. Per Cass., Sez. II, 20 maggio 2019, n. 21987, in *Giur. it.*, 2020, 1, 197 ss., i due reati non possono concorrere in quanto il reato di cui all'art. 615-*quater* costituirebbe necessario antefatto del reato di cui all'art. 615-*ter*. Al contrario per Cass., Sez. II, 25 settembre 2008, n. 36721 possono concorrere in quanto non sono tra loro in rapporto di specialità.

do così esplicito il rapporto di sussidiarietà tra tale norma incriminatrice e il più grave reato di indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti. Inoltre, il legislatore italiano ha specificato che gli oggetti del reato debbono essere «*costruiti principalmente per commettere tali reati, o specificamente adattati al medesimo scopo*». In tal modo, si è preso atto del fatto che molti dei programmi utilizzati per commettere reati possono avere finalità del tutto lecite e ha voluto selezionare i *software* oggettivamente configurati per commettere attività illecite, delimitando l'ambito del penalmente rilevante[15].

La stessa direttiva 2019/713/UE evidenziava la necessità di evitare una criminalizzazione di tali strumenti ove prodotti e posti in commercio per fini legittimi, sostenendo pertanto che la criminalizzazione dovrebbe essere limitata agli strumenti principalmente concepiti o specificamente adattati per la commissione dei comportamenti illeciti in essa richiamati[16].

L'introduzione di questa nuova fattispecie crea difficoltà applicative con riferimento ai rapporti col reato di cui all'art. 615-*quater* c.p.[17] Quest'ultimo, infatti, veniva ritenuto pacificamente applicabile, da parte della giurisprudenza, all'illecita acquisizione di codici di carte di credito e bancomat[18]. Questo perché il concetto di "parola chiave" è da sempre inteso come *password* o codice d'accesso, ovvero mezzo che permette di collegarsi al sistema[19]. Per cui tra gli «*altri mezzi idonei all'accesso*» si può includere anche l'indirizzo *e-mail* o il numero di carta di credito, ove svolgano le funzioni tipiche di identificazione dell'utente per abilitarlo all'accesso ai servizi *online*, normalmente abbinati con *password* o parole chiave.

La fattispecie di nuova introduzione, che si limita a far riferimento all' "uso nella commissione di reati" senza però specificare quali, si pone in rapporto

---

[15] Per approfondire la tematica dei c.d. *dual-use software* v. SALVADORI, *Il diritto penale dei software "a duplice uso"*, in *Diritto penale e modernità. Le nuove sfide tra terrorismo, sviluppo tecnologico e garanzie fondamentali*, a cura di Wenin-Fornasari, Napoli, 2017, 361 ss.

[16] V. i *considerando* n. 10 e 17 della direttiva.

[17] Per talune possibili frizioni v. con riferimento allo schema di attuazione del decreto legislativo VADALÀ, *La tutela penale della sicurezza degli scambi economici digitali*, Università degli Studi di Verona, Dipartimento di Scienze Giuridiche, 2021, 58 ss.

[18] Cfr. Cass., Sez. II, 3 ottobre 2013, n. 47021.

[19] FLOR, *Sub Art. 615-quater c.p.*, in *Commentario breve al codice penale*[6], a cura di Forti-Seminara-Zuccalà, Padova, 2017, 2134.

d'interferenza con l'art. 615-*quater* c.p. Poiché i due reati citati hanno pena identica, la clausola di sussidiarietà di cui all'art. 493-*quater* c.p. non risolve il conflitto. Inoltre, mentre al momento dell'introduzione della nuova fattispecie si poteva ritenere che gli oggetti dei due reati fossero differenti, oggi non è più così, perché, come si esaminerà in seguito, la L. 23 dicembre 2021, n. 238 ha ampliato l'oggetto del reato di cui all'art. 615-*quater* c.p., aggiungendovi proprio le "apparecchiature" e gli "strumenti" (nei quali possono dunque essere ricompresi i dispositivi o programmi informatici), che quindi viene a coincidere con quello di cui all'art. 493-*quater* c.p.

È difficile individuare allora un rapporto di specialità tra le due le fattispecie, perché appaiono strutturalmente molto differenti. L'oggetto del reato di cui all'art. 615-*quater* c.p. è più ampio perché ricomprende anche le mere *password* e i codici d'accesso. Inoltre, tali oggetti debbono essere specificamente idonei a consentire l'accesso ad un sistema informatico o telematico protetto da misure di sicurezza, non semplicemente essere strumenti per commettere reati come quelli di cui all'art. 493-*quater* c.p. Tuttavia, appare arduo tracciare il *discrimen* tra i due reati sulla base dell'idoneità o meno dell'apparecchio o programma informatico a consentire l'accesso abusivo, perché si tratta di una differenza assai labile. Infatti, nella maggior parte dei casi, per realizzare sia una frode informatica, sia una frode avente ad oggetto mezzi di pagamento diversi dai contanti è necessario realizzare un accesso abusivo al sistema informatico o telematico. Basti pensare all'*hacker* che creando un programma di tipo *spyware*, che poi invia alle sue potenziali vittime invitandole a cliccare su un *link* fasullo ed installa così il *malware* che intercetta le loro credenziali e gli consente di ottenere abusivamente l'accesso al loro sistema di *home banking*. Tale condotta, infatti, può astrattamente essere riconducibile ad entrambe le fattispecie. Va, però, evidenziato che l'elemento soggettivo dei due reati è diverso: infatti, nel caso dell'art. 615-*quater* c.p. è necessario che il fine criminoso sia quello di procurare a sé o ad altri un ingiusto profitto, mentre quello di cui all'art. 493-*quater* c.p. consiste nel fine di fare uso di tali strumenti nella commissione di reati.

Il *discrimen* tra le due fattispecie potrebbe essere individuato proprio nell'elemento soggettivo, anche se, all'atto pratico, appare difficile distinguere

i casi in cui il reo si procuri un dispositivo atto ad intercettare le credenziali altrui per trarne profitto, magari per venderle nel *darkweb*, oppure per commettere ulteriori reati concernenti i sistemi di pagamento. D'altra parte, pur non potendosi ritenere che tra le due fattispecie vi sia un rapporto di sussidiarietà per via della struttura molto differente dei due reati, non sembra neppure ragionevole ritenere che i due reati debbano necessariamente concorrere, pena un'ingiustificata duplicazione sanzionatoria.
L'oggetto materiale dell'art. 615-*quater* c.p. è più ampio, perché contempla anche le sole *password* e i codici d'accesso, per cui nel caso in cui il reo si limiti a disporre di codici e *password* si configurerebbe solo quest'ultima fattispecie. Per cui non appare giustificato che nel caso in cui il reo disponga di un programma di tipo *spyware* o di uno *skimmer,* invece del singolo codice d'accesso, debba rispondere di entrambi i reati.

3.3. *La nuova circostanza aggravante del reato di frode informatica.* Il nostro legislatore, con la novella del 2021, è intervenuto anche sul reato di frode informatica, inserendo una nuova circostanza aggravante «*se il fatto produce un trasferimento di denaro, di valore monetario o di valuta virtuale*». Essa è stata introdotta perché l'art. 6 della citata direttiva impone l'adozione di misure necessarie a sanzionare l'atto di effettuare o indurre un trasferimento di denaro, di 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, se commesso intenzionalmente ostacolando, senza diritto, il funzionamento di un sistema di informazione o interferendo con esso, oppure introducendo, alterando, cancellando, trasmettendo o sopprimendo senza diritto dati informatici. Il nostro legislatore ha ritenuto che tali condotte già rientrassero nell'ambito applicativo dell'art. 640-*ter* c.p. Tuttavia ha comunque deciso di introdurre la nuova circostanza aggravante allo scopo di «*riparametrare a quello dell'articolo 493-ter c.p. il regime sanzionatorio di tali condotte*»[20]. Si deve osservare, però, che i margini applicativi di quest'ultima circostanza aggravante finiscono per coincidere con quelli della fattispecie base, poiché la frode informatica è un reato di evento, che richiede

[20] V. la relazione illustrativa al d.lgs. 184/2021, disponibile *online* al sito www.camera.it.

si realizzi il danno per la vittima, danno che ha necessariamente connotazione patrimoniale, nonché un ingiusto profitto per sé o altri[21]. Poiché, dunque, ai fini della configurabilità della frode informatica non si può prescindere dalla concreta dimostrazione dell'avvenuto spostamento economico dalla vittima al reo, l'avvenuto "*trasferimento di denaro o valore monetario o valuta virtuale*" è già elemento costitutivo del reato. Pertanto, tale circostanza aggravante troverà applicazione alla totalità o quasi delle frodi informatiche. È infatti difficile anche solo immaginare una frode informatica che non abbia ad oggetto denaro o comunque un valore monetario. Dunque, più che inserire la suddetta circostanza aggravante, sarebbe stato più opportuno limitarsi ad aumentare la pena prevista per l'ipotesi base della frode informatica. Inoltre, la circostanza aggravante in questione fa specifico riferimento alla "valuta virtuale", contrapponendola al "valore monetario", senza, però, tener conto che, come specificato nell'art. 2 lett. d) della direttiva 2019/713/UE, anche la valuta virtuale è un mezzo di scambio: per cui, anche se non può essere classificato come moneta, ha comunque un suo valore economico. La stessa direttiva evidenzia che il suo ambito di applicazione dovrebbe essere limitato alle monete virtuali soltanto nella misura in cui possono essere comunemente utilizzate per effettuare pagamenti[22]. Dunque, il legislatore europeo sembra circoscrivere la tutela penale alla sola valuta che abbia una certa diffusione e caratteristiche tali da essere accettata da persone fisiche o giuridiche come mezzo di scambio. A maggior ragione non si comprende quindi il motivo della contrapposizione tra i due concetti.

4. *Le modifiche al d.lgs. 8 giugno 2001, n. 231 in materia di responsabilità da reato delle persone giuridiche e gli ulteriori interventi normativi.* Con il d.lgs. n. 184/2001, il nostro legislatore è intervenuto anche in materia di responsabilità da reato degli enti, introducendo il nuovo articolo 25-*octies*.1, che sanziona l'ente nel cui interesse o vantaggio sono stati commessi i reati di cui agli artt. 493-*ter* c.p. 493-*quater* e 640-*ter* c.p. aggravato dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale. Nel fare

[21] PICA, *Diritto penale delle tecnologie informatiche*, Torino, 1999, 148 ss.
[22] V. *Considerando* n. 10.

questo il legislatore italiano ha adempiuto agli obblighi previsti dall'art. 10 della direttiva 2019/713/UE, che impone agli Stati membri di adottare le misure necessarie affinché le persone giuridiche siano ritenute responsabili dei fatti illeciti richiamati dalla direttiva.

Sebbene non si possa che accogliere favorevolmente l'introduzione del nuovo art. 25-*octies*.1, risulta di difficile comprensione la motivazione per la quale il legislatore non abbia semplicemente inserito la fattispecie base di cui all'art. 640-*ter* c.p. nel catalogo dei reati presupposto, come sarebbe stato auspicabile[23]. Dal momento che la nuova circostanza aggravante finisce fondamentalmente per coincidere con l'evento della fattispecie base, si potrebbe ritenere che la frode informatica ora rientri sostanzialmente nel catalogo dei reati presupposto.

Inoltre, al co. 2 dell'art. 25-*octies*.1 cit. è stato previsto un nuovo illecito amministrativo sussidiario in caso di commissione di ogni altro delitto contro la fede pubblica, contro il patrimonio o che comunque offende il patrimonio previsto dal codice penale, avente ad oggetto strumenti di pagamento diversi dai contanti. Poiché la frode informatica è un reato contro il patrimonio e per la sua struttura ha necessariamente ad oggetto strumenti di pagamento diversi dai contanti, a maggior ragione si può ritenere che quest'ultima ipotesi sia a tutti gli effetti ricompresa nel catalogo dei reati presupposto per la responsabilità amministrativa da reato degli enti.

Ulteriore importante modifica riguarda la disciplina della confisca. Il d.lgs. n. 184/2021 ha inserito all'art. 493-*quater* c.p. un nuovo secondo comma, che prevede la confisca «*delle apparecchiature, dei dispositivi o dei programmi informatici*» nonché quella «*del profitto o del prodotto del reato*», anche per equivalente. In questo caso si è trattato di un'autonoma scelta del nostro legislatore, in quanto la direttiva non prevedeva alcun obbligo di confisca per tali attività. La norma ricalca pedissequamente il disposto dell'art. 493-*ter*, c. 2, c.p., tuttavia senza prevedere la clausola di salvaguardia, per cui la confisca del profitto o del prodotto del reato non può essere disposta quando questi siano appartenenti a persona estranea al reato. Proprio per questa rilevante omis-

[23] In tal senso BELTRANI, *Reati informatici e d.lgs. 231/2001 alla luce della legge di attuazione della Convenzione di Budapest*, in *Resp. amm. società e degli enti*, 2008, 4, 21.

sione, come osservato dai primi commentatori, questa disparità di trattamento non è giustificata[24]. Effettivamente, non si comprende perché il profitto derivante ad esempio dalla vendita di *software* con codici sorgenti maligni sia confiscabile anche ove ne risulti titolare un terzo estraneo al reato, mentre ciò non sia possibile per il profitto derivante dall'effettivo utilizzo di tale *software*.
Il d.lgs. 184/2021 ha introdotto altresì diverse disposizioni, che pur avendo natura extra-penale, hanno notevole rilevanza, perché volte a garantire un'efficace cooperazione internazionale nel contrasto ai reati commessi contro gli strumenti di pagamento diversi dai contanti. Infatti, in ottemperanza agli obblighi previsti dalla direttiva, l'art. 4 prevede la raccolta di dati statistici sulle frodi e sulle falsificazioni relative a strumenti di pagamento diversi dai contanti. In particolare, si prevede la raccolta di dati relativi al numero dei procedimenti iscritti e dei procedimenti definiti con sentenza di condanna per reati aventi ad oggetto strumenti di pagamento diversi dai contanti, nonché al numero delle persone indagate e al numero delle persone condannate per i medesimi reati. Questa è una disposizione significativa, perché ad oggi nelle statistiche giudiziarie le frodi informatiche vengono conteggiate assieme alle truffe comuni, mentre i reati di indebito uso e falsificazione di carte di credito e di pagamento non sono neppure inseriti in una categoria a sé stante, bensì indicati alla voce "*altri reati*"[25]. La raccolta di specifici dati aggiornati consente invece il loro scambio con organismi quali la Commissione europea, Europol ed Eurojust, anche ai fini di una miglior cooperazione tra i diversi Stati membri. Proprio a tal fine il successivo art. 5 del d.lgs. cit. individua nella Sala operativa internazionale, incardinata nel Servizio per la cooperazione internazionale di polizia della Direzione centrale della polizia criminale, il punto di contatto operativo nazionale per lo scambio di informazioni raccolte e richieste dalle autorità di altro Stato membro relative ai reati di cui al nuovo decreto.

[24] BERNARDONI, *op. cit.*
[25] V. dati dell'Istituto Nazionale di statistica relativi all'anno 2019 con riguardo alla tipologia di reati commessa, ai delitti di cui si è scoperto l'autore e dei condannati con riferimento alla natura del reato, disponibili *online* al sito www.dati.istat.it.

5. L'attuazione della direttiva 2013/40/UE, relativa agli attacchi contro i sistemi di informazione. Con l'art. 19 della L. 23 dicembre 2021, n. 238, ovvero la c.d. legge europea 2019-2020 per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea, il nostro legislatore ha apportato diverse modifiche agli artt. 615-*quater*, 615-*quinquies*, 617, 617-*bis*, 617-*quater* e 617-*quinquies* del codice penale, al fine di adeguarli al disposto della Direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione.
L'*iter* legislativo per l'attuazione di tale direttiva è stato particolarmente travagliato: inizialmente, infatti, il legislatore italiano aveva comunicato alla Commissione europea che non vi era necessità di specifici interventi per attuare la direttiva, sostenendo che l'ordinamento nazionale fosse già conforme alle sue disposizioni[26]. Tuttavia, la Commissione ha ritenuto che così non fosse ed ha aperto una procedura d'infrazione contro il nostro Paese per il mancato recepimento di tale normativa entro il termine previsto[27]. Il legislatore italiano, dunque, ha deciso di intervenire con la citata legge europea 2019-2020.
A differenza di quanto avvenuto per il recepimento della direttiva 2019/713/UE, il legislatore si è qui limitato ad intervenire unicamente sul testo norme incriminatrici già in vigore nel codice penale, in alcuni casi modificando la formulazione del fatto tipico e ampliando l'oggetto materiale del reato, e a rimodulare, in alcuni casi, il trattamento sanzionatorio.
Nulla è stato previsto in materia di responsabilità da reato delle persone giuridiche, nonostante l'obbligo previsto dall'art. 11 della direttiva in tal senso. Tuttavia, si evidenzia che l'art. 24-*bis* del d.lgs. 8 giugno 2001, n. 231 già prevede quali reati presupposto per la responsabilità dell'ente i delitti di cui agli artt. 615-*quater*, 615-*quinquies*, 617-*quater* e 617-*quinquies* c.p. Inoltre, diversamente da quanto imposto dalla predetta direttiva, non è stata prevista alcuna disposizione in merito allo scambio di informazioni tra le autorità degli

[26] V. Dossier n. 294/2 del 13 aprile 2021, *Scheda di lettura della legge europea 2019- 2021* a cura dei Servizi e degli Uffici del Senato della Repubblica e della Camera dei deputati, disponibile *online* al seguente link: https://www.senato.it/japp/bgt/showdoc/18/DOSSIER/0/1210765/index.html?part=dossier_dossier1-frontespizio_front01, 82 ss.
[27] Ovvero il 4 settembre 2015. Per il mancato rispetto di tale termine è stata aperta la procedura di infrazione n. 2019/2033.

Stati membri e alla predisposizione di statistiche sull'incidenza dei reati di cui alla direttiva.

5.1. *Le modifiche apportate ai reati contro la riservatezza informatica.* La prima modifica apportata dall'art. 19 L. n. 238/2021 riguarda il delitto di detenzione e diffusione abusiva di codici e altri mezzi atti all'accesso a sistemi informatici o telematici di cui all'art. 615-*quater* c.p. Tale fattispecie legale è stata innovata sotto molteplici aspetti, a partire dalla sua rubrica, che ora si intitola «*detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici*». L'oggetto del reato è stato ampliato, per cui oggi ricomprende non solo i codici, le parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, ma anche «*apparati, strumenti, parti di apparati o strumenti*». A ben guardare, però, anche tali oggetti già potevano rientrare nella clausola di chiusura eccessivamente elastica già richiamata dal precetto. Anzi, questa modifica paradossalmente complica il lavoro degli interpreti, perché la direttiva fa riferimento alle diverse nozioni di "*sistema di informazione*" e "*dati informatici*"[28]. In ogni caso la giurisprudenza già in passato aveva evidenziato la loro natura di categorie aperte e dinamiche, suscettibili di essere adeguate per effetto delle innovazioni tecnologiche[29]. Si ritiene, dunque, che gli apparati altro non siano che apparecchiature per accedere al sistema informatico, mentre gli strumenti devono essere equiparati ai *software*[30].
Alle condotte sanzionate sono state aggiunte, oltre alla "*detenzione*", così da adeguare finalmente il contenuto della norma alla sua rubrica[31], nonché

[28] V. FUMO, *La condotta nei reati informatici*, in *questa Rivista*, 2013, 3, 775 ss., che critica l'utilizzo da parte del legislatore in quest'ambito di termini "vaghi e indeterminati", spesso erroneamente tradotti dalla lingua inglese.
[29] Cass. pen., sez. V, sentenza 5 aprile 2019, n. 15071.
[30] V. la relazione n. 20/2022 dell'Ufficio del Massimario della Corte di cassazione, 6.
[31] Prima di tale modifica era dibattuto in dottrina se la mera detenzione di codici di accesso fosse sanzionata o meno dalla norma. In senso favorevole v. MANTOVANI, *Diritto pen*ale. *Parte speciale*[3], I, Padova, 2019, 622; CANNATA-COSTALUNGHI, *Detenzione e diffusione di codici d'accesso a sistemi informatici o telematici (art. 615-quater)*, in *Trattato di diritto penale. Parte speciale*, IX, *I delitti contro la libertà sessuale, la libertà morale, l'inviolabilità del domicilio e l'inviolabilità dei segreti*, a cura di Cadoppi-Canestrari-Manna-Papa, Torino, 2011, 555. In senso contrario v. SALVADORI, *I reati contro la riservatezza informatica*, cit., 694 ss. e PARODI, *I reati patrimoniali*, in *Diritto penale dell'informatica. Reati della rete e sulla rete*, a cura di Parodi-Sellaroli, Milano, 2020, 147.

"*l'installazione*" e la "*messa in altro modo a disposizione di altri*" di strumenti o dispositivi idonei ad accedere ad un sistema informatico o telematico protetto da misure di sicurezza. L'art. 19 L. cit. ha aumentato la pena detentiva per il reato base, che ora è punito con la reclusione sino a due anni. Le modifiche hanno riguardato anche le circostanze aggravanti: il precedente richiamo di cui al co. 2 dell'art. 615-*quater* c.p. alle ipotesi aggravate di cui all'art. 617-*quater* c.p. è stato ampliato sino a ricomprendere l'ipotesi del fatto commesso da chi esercita abusivamente la professione di investigatore privato. Inoltre, il massimo edittale delle ipotesi aggravate è stato elevato a tre anni di reclusione. Per quanto riguarda l'aggiunta della "*detenzione*" alle condotte sanzionate, dev'essere subito evidenziato che si è trattata di una scelta autonoma del legislatore italiano, in quanto la direttiva 2013/40/UE non prevede l'obbligo per gli Stati di incriminare tale ipotesi. Tale inserimento presenta notevoli problematiche, in quanto è difficile accertare quando l'utente abbia l'effettiva disponibilità degli oggetti indicati[32]. In particolare, il problema principale è lo stesso che si pone per la detenzione di materiale pedopornografico: ovvero se la mera accessibilità possa in quel caso essere equiparata a un "possesso" penalmente rilevante[33]. Se non vi è dubbio che il salvataggio dei dati della *cache* integri il fatto materiale del possesso, anche in caso di successiva cancellazione[34], questo non è altrettanto pacifico per quei casi in cui l'utente si limiti a visualizzare la pagina *Internet* e questa venga automaticamente salvata dal *browser* nei *file* temporanei. Infatti, se non sempre l'utente è a conoscenza del salvataggio automatico di tali dati, però può comunque disporne, dato che è sufficiente accedere alla cartella dei *download* per consultare tali file. La Cassazione in materia di detenzione di materiale pedopornografico ha ritenuto che anche il collocamento di file contenenti materiale pedopornografico nel "cestino" del sistema operativo del *computer* integri la condotta di detenzione, perché questi restano comunque disponibili mediante la semplice riat-

[32] SALVADORI, *I reati di possesso. Un'indagine dogmatica e politico-criminale in prospettiva storica e comparata*, Napoli, 2016, 85.
[33] *Ibid.*, 86 ss.
[34] Cass., Sez. III, 29 novembre 2021, n. 43615; Cass., Sez. III, 19 marzo 2021, n. 10759; Cass., Sez. III, 14 gennaio 2019, n. 1509; Cass., Sez. III, 8 marzo 2017, n. 11044.

tivazione dell'accesso al *file*[35]. Il *file* automaticamente scaricato nel computer resta comunque a disposizione dell'utente, che lo può in qualsiasi momento trovare nell'apposita cartella e aprire, si può ritenere che si configuri il reato in esame. In caso di mancata conoscenza dell'avvenuto trasferimento va però tenuto presente che la norma richiede, oltre alla "volontà consapevole" di procurarsi, produrre, detenere, cedere o altrimenti mettere a disposizione c.d. *hacking-tools*, il dolo specifico del «*fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno*»: per cui difetterebbe comunque l'elemento soggettivo e non si configurerebbe un possesso penalmente rilevante[36].

Con l'aggiunta della "detenzione" alle condotte punibili il legislatore ha scelto di sanzionare anche coloro che, senza essersi procurati o senza farne uso, si limitino a disporre dei dispositivi elencati, idonei all'accesso al sistema informatico.

L'estensione dell'ambito applicativo della norma presenta alcune criticità anche sotto il profilo del rispetto dei principi di offensività e di proporzione[37]. È evidente che lo scopo politico-criminale di questa incriminazione è quello di impedire l'utilizzo dei menzionati oggetti, detenuti per commettere un più grave reato, in specie l'accesso abusivo al sistema informatico o telematico, il quale a sua volta può preludere alla commissione di ulteriori illeciti. Tuttavia, la detenzione è di per sé una condotta c.d. neutra, che non presenta disvalore sociale[38]. La previsione del fine criminoso viene pertanto ad assolvere una funzione fondatrice o costitutiva dei comportamenti penalmente illeciti rispetto a quelli leciti. In tal senso, la condotta oggettiva rappresenta un "mezzo" strumentale al perseguimento del fine soggettivamente tipizzato[39]. Il rischio è che l'elemento soggettivo finisca inammissibilmente per essere presunto sulla base della mera presenza dei dati all'interno del sistema informatico.

---

[35] Cass., Sez. III, 29 novembre 2021, n. 43615, cit.; Cass., Sez. III, 21 aprile 2015, n. 24345; Cass., Sez. III, 6 ottobre 2010, n. 639.

[36] In tal senso anche SALVADORI, *I reati di possesso*, cit., 87 s.

[37] V. PECORELLA, *Diritto penale dell'informatica*[2], Padova, 2006, 359 ss., che già nella sua vecchia formulazione riteneva l'art. 615-*quater* c.p. «*difficilmente conciliabile col principio di proporzione*» in ragione dell'eccessiva anticipazione della tutela penale. Negli stessi termini anche FUMO, *op. cit.*, 782.

[38] SALVADORI, *I reati di possesso*, cit., 101.

[39] PICOTTI, *Il dolo specifico*, cit., 501.

Già nella sua precedente formulazione l'art. 615-*quater* c.p. conteneva la clausola d'illiceità speciale dell'abusività delle condotte, abusività che viene solitamente intesa come contrarietà alle norme extrapenali che disciplinano l'attività dei soggetti che operano nel settore informatico[40]. Il carattere abusivo conferisce alla detenzione una speciale connotazione negativa, arricchendo il fatto tipico qualificandolo in termini oggettivi. Pertanto, rispetto a tale ipotesi criminosa, oltre al dolo specifico richiesto dalla norma, che, però, non riesce a delimitare adeguatamente l'ambito del penalmente rilevante[41], è necessaria anche la consapevolezza del carattere penalmente illecito della detenzione di un determinato oggetto tra quelli indicati dall'art. 615-*quater* c.p. e del suo disvalore per un interesse giuridico, che presuppone la conoscenza attuale della normativa extrapenale di riferimento. Tale elemento essenziale, che concorre a descrivere il fatto di reato, deve rientrare nell'oggetto del dolo. Pertanto, dovrebbero essere escluse inammissibili presunzioni di colpevolezza.

Da apprezzare è la scelta di aggiungere, nella descrizione del fatto tipico, la condotta di"installazione" alle condotte sanzionate, data l'ampia diffusione delle *App* di autenticazione per l'accesso a determinati servizi *online*, così come della clausola di chiusura «*mette in altro modo a disposizione di altri*», che permette di ricondurre nell'ambito applicativo della fattispecie i comportamenti che consistono nel mettere a disposizione con qualsiasi modalità *file* e dati e quindi anche qualsiasi mezzo idoneo all'accesso al sistema informatico o telematico.

Una nota critica, infine, riguarda la scelta del legislatore di non inserire alcuna clausola di sussidiarietà all'interno dell'art. 615-*quater* c.p., lasciando così irrisolto il problema relativo all'individuazione dei rapporti tra quest'ultima fattispecie e l'art. 615-*ter* c.p.[42]

L'art. 19 L. 238/2021 ha poi modificato in modo significativo anche l'art. 615-*quinquies* c.p., la cui rubrica è ora intitolata «*detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a*

[40] PICOTTI, *Internet e diritto penale: il quadro attuale alla luce dell'armonizzazione internazionale*, in *Dir. dell'Internet*, 2005, 2, 197; SALVADORI, *I reati contro la riservatezza informatica*, cit., 696.
[41] SALVADORI, *I reati contro la riservatezza informatica*, cit., p. 696.
[42] V. *supra*, n. 13.

danneggiare o interrompere un sistema informatico o telematico». Alle condotte precedentemente sanzionate dalla norma sono state aggiunte la "*detenzione*" e l'"*installazione*" degli oggetti ivi indicati, mentre la "*messa a disposizione di altri*" è stata ampliata tramite l'aggiunta della locuzione espansiva "*in qualsiasi modo*".

Per quanto riguarda la critica all'aggiunta della mera detenzione alle condotte sanzionate, si richiama quanto già indicato con riferimento all'art. 615-*quater* c.p. Ulteriore modifica consiste nell'aggiunta dell'avverbio "*abusivamente*", per cui ora la formulazione della norma incriminatrice è in parte analoga a quanto previsto dall'art. 615-*ter* c.p.

Per quanto riguarda il nuovo requisito dell'abusività, in mancanza di un inciso analogo a quello di cui all'art. 615-*ter* c.p., che punisce la condotta di mantenimento in un sistema informatico o telematico protetto da misure di sicurezza «*contro la volontà espressa o tacita di chi ha il diritto di escluderlo*», non si può aderire alla tesi per cui tale richiamo sarebbe pleonastico[43] e si deve invece ritenere che costituisca una clausola d'illiceità speciale[44]. In questo modo, il legislatore ha voluto specificare che la detenzione, la diffusione, l'installazione e tutte le altre condotte descritte sono di per sé lecite, ma diventano penalmente rilevanti se "*abusive*", vale a dire se poste in essere "senza autorizzazione".

Per individuare quando la condotta tipica sia abusiva, in mancanza di altri elementi, si potrebbe fare riferimento al concetto di "*abusività*" elaborato con riguardo all'art. 615-*ter* c.p., che ha dato origine ad un rilevante conflitto giurisprudenziale[45]. In tal senso, si dovrebbe stabilire se l'abusività corrisponda soltanto all'assenza di necessaria autorizzazione[46], oppure anche come violazione

---

[43] PICA, *op. cit.*, 38 ss.; GATTA, *Delitti contro l'inviolabilità del domicilio*, in *Trattato teorico/pratico di diritto penale*, VII, *Reati contro la persona e contro il patrimonio*[3], a cura di Viganò-Piergallini, Torino, 2015, 353.

[44] SALVADORI, *I reati contro la riservatezza informatica*, cit., 617; Relazione n. 20/2022 dell'Ufficio del Massimario della Corte di cassazione cit., 8.

[45] Sono ben due le pronunce delle Sezioni Unite sul punto, ovvero Cass., Sez. un., 27 ottobre 2011, n. 4694, in *Cass. pen.*, 2012, 11, 3681 ss. e Cass., Sez. un., 8 settembre 2017, n. 41210, in *Cass. pen.*, 2018, 2, 509 ss.

[46] Così FLOR, *Verso una rivalutazione dell'art. 615-ter c.p.? Il reato di accesso abusivo a sistemi informatici o telematici fra la tutela di tradizionali e di nuovi diritti fondamentali nell'era di Internet*, in *Dir. pen. cont.*, 2012, 2, 128.

dei suoi limiti[47]. A tal proposito, va rilevato che l'art. 5 della direttiva 2013/40/UE prevede l'incriminazione delle condotte di interferenza illecita relativamente ai dati a condizione che le stesse siano compiute «*intenzionalmente e senza diritto*», ove il concetto di "*senza diritto*" viene definito alla lett. d) dell'art. 2 della medesima direttiva come mancanza di autorizzazione da parte del titolare del sistema[48]. In questo caso, dunque, poiché l'intervento legislativo in questione aveva come finalità proprio l'adempimento della direttiva, la locuzione "senza diritto" sembra costituire il perno su cui ruota il disvalore del precetto: per cui l'abusività della condotta dovrebbe coincidere con la sola assenza di autorizzazione e non anche con la violazione dei limiti. Non a caso, il nuovo art. 615-*quinquies* c.p., a differenza dell'art. 615-*ter* c.p., menziona solo l'"*abusività*" e non anche la mancanza del consenso, a riprova della volontà legislativa di non dilatare eccessivamente l'ambito applicativo della fattispecie.

L'art. 19 L. cit. ha poi completamente riscritto il co. 1 dell'art. 617-*bis* c.p. e sostituito la sua rubrica con la seguente: «*detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni o conversazioni telegrafiche o telefoniche*». Tale reato ora punisce le condotte consistenti nel procurarsi, detenere, produrre, riprodurre, diffondere, importare, comunicare, consegnare, mettere in altro modo a disposizione di altri o nell'installare apparati, strumenti o parti di apparati o di strumenti idonei a intercettare, impedire o interrompere comunicazioni o conversazioni telefoniche o telegrafiche tra altre persone. Dunque, la tutela della riservatezza e della libertà delle comunicazioni è stata ulteriormente anticipata, perché addirittura si sanzionano condotte prodromiche o preparatorie all'installazione delle apparecchiature. Per quanto riguarda l'elemento soggettivo, è rimasto il dolo specifico[49], ma il fine richiesto non è

[47] In tal senso SALVADORI, *Quando un insider accede abusivamente ad un sistema informatico o telematico? Le Sezioni Unite precisano l'ambito applicazione dell'art. 615-ter c.p.*, in *Riv. trim. dir. pen. econ*, 2012, 1-2, 369 ss.

[48] L'art. 2 lett. d) della Direttiva 2013/40/UE fornisce la seguente definizione di "senza diritto": «*Una condotta di cui alla presente direttiva, ivi inclusi l'accesso, l'interferenza o l'intercettazione, che non è autorizzata da parte del proprietario o da un altro titolare di diritti sul sistema o su una sua parte, ovvero non consentiti a norma del diritto nazionale*».

[49] PERRI, *Sub art. 617-bis c.p.*, in *Commentario breve al codice penale*[6], a cura di Forti-Seminara-

più quello di porre in essere l'attività di intercettazione o di interruzione di comunicazioni o conversazioni, essendo ora sufficiente che il reo agisca «*al fine di prendere cognizione di una comunicazione o di una conversazione telefonica o telegrafica tra altre persone o comunque a lui non diretta, ovvero di impedirla o di interromperla*». Anche in questo caso suscita notevoli perplessità l'aggiunta della mera "*detenzione*" alle condotte sanzionate, a maggior ragione dato che in questo caso non vi è neppure una clausola d'illiceità speciale, in quanto la norma si limita a prevedere la locuzione «*al di fuori dei casi consentiti dalla legge*», mera ipotesi d'illiceità espressa[50]. Dunque, il dolo specifico ha un ruolo fondamentale, posto che, come detto, il procurarsi e il detenere sono condotte neutre. Vi è quindi il rischio concreto che si verifichino inammissibili presunzioni di colpevolezza sulla base del mero possesso di uno degli oggetti indicati dalla norma.

Anche la rubrica dell'art. 617-*quinquies* c.p. è stata sostituita e ora è intitolata «*Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche*». Il novero delle condotte punibili è stato notevolmente ampliato: rispetto all'iniziale sola "*installazione*" oggi si sanziona anche colui che «*si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri*». Anche in questo caso la tutela penale è stata notevolmente anticipata rispetto alla stessa installazione.

Tra gli oggetti del reato sono stati ricompresi anche programmi informatici, codici, parole chiave o altri mezzi atti ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi. Queste modifiche rendono questo reato simile al novellato art. 617-*bis* c.p., da cui diverge in quanto quest'ultimo tutela le comunicazioni e le conversazioni telegrafiche o telefoniche tra persone, mentre quello di cui all'art. 617-*quinquies* c.p. le comunicazioni informatiche o telematiche tra sistemi. Inoltre, a seguito dell'ampiamento del numero degli oggetti atti a integrare il reato di cui all'art. 617-*quinquies* c.p., non vi è più quel

---

Zuccalà, Padova, 2017, 2145.

[50] PULITANÒ, *Illiceità espressa e illiceità speciale*, in *Riv. it. dir. proc. pen.*, 1967, 74 ss.

"restringimento" rispetto all'analoga previsione di cui all'art. 617-*bis* c.p. che era stato evidenziato da una parte della dottrina[51]. Il legislatore italiano è intervenuto anche sull'elemento soggettivo, aggiungendo la locuzione «*al fine di intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle*». In questo modo ha posto fine al dibattito dottrinale esistente in merito[52], poiché con l'espressa enunciazione del fine criminoso non vi sono più dubbi sul fatto che l'elemento soggettivo richiesto dall'art. 617-*quinquies* c.p. sia il dolo specifico.
Le modifiche agli artt. 617 e 617-*quater* c.p. hanno riguardato unicamente il trattamento sanzionatorio e sono state aumentate le pene previste sia per la fattispecie base che per le ipotesi aggravate. Resta pertanto irrisolto il problema relativo alla possibilità di concorso tra i reati di cui agli artt. 617-*quater* e 617-*quinquies* c.p. Se si ritenesse applicabile unicamente il criterio della specialità, si dovrebbe necessariamente concludere che le due fattispecie concorrano tra loro, perché si consumano in momenti differenti[53]. Tuttavia, a ben guardare, non si può che constatare come per intercettare una comunicazione sia necessario quantomeno installare un'"apparecchiatura" che consenta di fare ciò. Di conseguenza, l'art. 617-*quinquies* c.p. si pone quale necessario antefatto rispetto all'art. 617-*quater* c.p. Pertanto, anche per evitare duplicazioni sanzionatorie, sarebbe opportuno considerare l'art. 617-*quinquies* c.p. assorbito nel reato di cui all'art. 617-*quater* c.p.[54]. Va, però, evidenziato che un rilevante ostacolo all'assorbimento è rappresentato dal trattamento sanzionatorio particolarmente elevato dell'art. 617-*quinquies* c.p.
A tutt'oggi né l'art. 617 né l'art. 617-*bis* c.p. sono inclusi nel catalogo dei reati presupposto di cui al d.lgs. 231/2001. Poiché l'art. 10 della direttiva 2013/40/UE obbliga gli Stati membri ad adottare tutte le misure per assicurare la punibilità delle persone giuridiche per la commissione di uno qualsiasi

[51] PERRI, *Sub art. 617-quinquies c.p.*, in *Commentario breve al codice penale*, cit., 2151.
[52] Secondo un primo orientamento il reato era punito a titolo di dolo generico, poiché non vi era l'enunciazione di alcun fine, v. SALVADORI, *I reati contro la riservatezza informatica*, cit., 714. *Contra* v. PECORELLA, *op. cit.*, 305.
[53] Favorevole alla tesi del concorso è PERRI, *Sub art. 617-quater c.p.*, in *Commentario breve al codice penale*, cit., 2150.
[54] In tal senso anche Cass., Sez. V, 29 gennaio 2016, n. 4059, che evidenzia come si tratti di una progressione criminosa.

degli atti illeciti ivi descritti, commessi nel loro interesse o vantaggio, questa "dimenticanza" da parte del nostro legislatore rende ancora una volta la legge nazionale di attuazione non pienamente conforme agli obblighi di incriminazione europei.

L'art. 4 della direttiva 2013/40/UE prevedeva espressamente l'incriminazione delle condotte di "*ostacolare gravemente o interrompere il funzionamento di un sistema di informazione*", compiute anche "*rendendo inaccessibili i dati informatici*". Tuttavia, l'art. 19 della citata direttiva non ha aggiunto tali condotte in nessuna delle fattispecie elencate, nonostante la Commissione europea avesse già nel 2017 evidenziato che la normativa italiana in materia non rispettava il contenuto della Direttiva[55].

Il co. 3 dell'art. 420 c.p., che puniva l'ipotesi aggravata del delitto di "attentato informatico" qualora dal fatto di reato fosse derivata l'interruzione, anche parziale, del funzionamento dell'impianto o del sistema informatico attaccato, è stata abrogata dalla L. 18 marzo 2008, n. 48[56], recante la rettifica e la attuazione della Convenzione sul cybercrime del Consiglio d'Europa del 2001. Inoltre, gli odierni artt. 635-*quater* e 635-*quinquies* c.p. non fanno alcun riferimento all'interruzione o al fatto di rendere inaccessibili i dati. Dunque, è opportuno che il legislatore intervenga quanto prima per introdurre (o reintrodurre[57]) la punibilità delle condotte in esame, data la massiccia diffusione dei *malware* di tipo *ransomware*, volti proprio ad impedire agli utenti di accedere liberamente al proprio sistema informatico, se non a seguito del pagamento di un riscatto.

---

[55] *Relazione della Commissione al Parlamento europeo e al Consiglio che valuta in che misura gli Stati membri hanno adottato le misure necessarie per conformarsi alla direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio*, disponibile *online* al sito https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52017DC0474&qid=1506754119753&from=IT

[56] Per approfondire v. PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto penale sostanziale*, in *Dir. pen. proc.*, 2008, 6, 700 ss.; SALVADORI, *Il "microsistema" normativo concernente i danneggiamenti informatici, un bilancio molto poco esaltante*, in *Riv. it. dir. proc. pen.*, 2012, 1, 204 ss.

[57] Come sostenuto anche da CIVELLO 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*, 30 ottobre 2013, 4.

6. *Le criticità irrisolte: la mancata previsione di disposizioni relative alla giurisdizione e il coordinamento tra le diverse norme incriminatrici.* Sia la direttiva 2019/713/UE, all'art. 12, che la direttiva 2013/40/UE, sempre all'art. 12, obbligano gli Stati membri ad adottare «*le misure necessarie a stabilire la propria giurisdizione per i reati di cui agli articoli da 3 a 8*». Tuttavia, in entrambi i casi il legislatore italiano nulla ha previsto in materia di giurisdizione, lasciando così irrisolti tutti i problemi esistenti relativi all'individuazione del giudice competente[58].

La procedura d'infrazione aperta per il mancato recepimento della direttiva 2013/40/UE riguardava proprio quest'ultimo profilo, ovvero la mancata attuazione delle disposizioni relative alla giurisdizione[59]. Dunque, anche per questo aspetto il legislatore italiano non ha recepito correttamente la direttiva europea ed è assai probabile che in futuro vi saranno ulteriori contestazioni.

Una soluzione poteva essere quella di prevedere espressamente la giurisdizione italiana qualora la vittima risieda in territorio italiano, il che avrebbe certamente giovato alla speditezza dei procedimenti: ma tale facoltà è stata riconosciuta dalla sola direttiva 2019/713/UE, previa comunicazione alla Commissione europea. È però vero che la lett. b) dell'art. 12 della direttiva prevede che lo Stato membro è tenuto ad assicurare la propria competenza giurisdizionale nel caso in cui il reato sia stato commesso contro un sistema di informazione 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. Dunque, nulla vieta di fare riferimento alla collocazione del sistema informatico oggetto di attacco, ed indirettamente così al luogo in cui risiede la vittima. Pertanto, si auspica un nuovo intervento normativo volto a correggere tale inottemperanza.

Inoltre, la direttiva 2013/40/UE all'art. 9 par. 5 prevede che qualora i fatti da essa contemplati dagli artt. 4 e 5, che riguardano rispettivamente l'ostacolo e l'interruzione del funzionamento di un sistema di informazione, nonché il danneggiamento di dati informatici, siano commessi abusando dei dati perso-

[58] FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in *Cybercrime*, a cura di Cadoppi-Canestrari-Manna-Papa, Torino, 2019, 191.
[59] Dossier n. 294/2, cit., 84.

nali 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. Il legislatore italiano, tuttavia, non ha accolto tale invito del legislatore europeo, nonostante le raccomandazioni di quest'ultimo[60].

L'art. 9 par. 5 cit. prevede tale possibilità «*purché tale circostanza non sia già contemplata da un altro reato punibile a norma del diritto nazionale*». Il co. 3 dell'art. 640-*ter* c.p. già prevede la circostanza aggravante della frode informatica commessa con furto o indebito utilizzo dell'identità digitale, tale scelta non costituisce una violazione della direttiva in esame. Tuttavia, poiché l'inciso sopra riportato non sembra configuri un vero e proprio divieto, si ritiene che il legislatore italiano ben avrebbe potuto intervenire in tal senso aggiungendo un'ulteriore circostanza aggravante e in questo modo rafforzare la tutela dell'identità digitale.

Un profilo che suscita particolare criticità è che l'attuazione di tali direttive è avvenuta con atti legislativi separati. Nell' ordinamento italiano lo sviluppo di una normativa in materia di criminalità informatica è avvenuto senza un previo disegno sistematico, ovvero in modo disorganico e frammentario[61] e anche in quest'occasione il legislatore non ha fatto eccezione. Sebbene ciascuno dei due provvedimenti attuativi ha riguardato reati posti a tutela di beni giuridici diversi ed ha seguito la collocazione sistematica delle norme incriminatrici che si volevano modificare, si sarebbe, però, dovuto tener conto che le fattispecie a protezione del bene giuridico della riservatezza informatica si presentano spesso come complementari rispetto ai delitti di frode informatica e di falsificazione di mezzi di pagamento.

Nella maggioranza dei casi gli attacchi informatici si articolano in una pluralità di fasi strettamente concatenate tra loro. Basti pensare al fatto che prima di riuscire ad inserirsi nel sistema di *home banking* della vittima, il reo ha prima necessità quantomeno di carpire le sue credenziali o facendosele consegnare

[60] V. il *Considerando* n. 14 della predetta direttiva, nel quale si raccomanda l'istituzione di efficaci misure contro il furto d'identità e altri reati connessi all'identità.

[61] PICOTTI, *Sistematica*, cit., 22; PECORELLA, *op. cit.*, 3 ss.

dalla stessa vittima in modo fraudolento tramite la tecnica del *phishing* classico oppure installando un *virus* di tipo *spyware* sul suo computer[62].

La direttiva 2013/40/UE[63] ha evidenziato che gli attacchi informatici su larga scala possono causare ingenti danni economici sia attraverso l'interruzione dei sistemi di informazione e delle comunicazioni, sia attraverso la perdita o l'alterazione di informazioni riservate commercialmente importanti o di altri dati. Allo stesso tempo, la direttiva 2019/713/UE sottolinea la connessione tra gli attacchi ai sistemi di informazione e archiviazione dei dati e le aggressioni patrimoniali: infatti, nella scelta delle condotte da incriminare, si propone come scopo proprio quello di integrare e rafforzare la direttiva 2013/40/UE[64].

Gli attacchi ai sistemi di informazioni e le frodi e falsificazioni dei mezzi di pagamento diversi dai contanti non sono affatto scollegati tra di loro. Per questo motivo sarebbe stata più opportuna un'unica riforma che, attuando entrambe le direttive, intervenisse in modo omogeneo per attuare un sistema coerente. Quantomeno, data la brevissima distanza tra l'adozione dei due provvedimenti legislativi, il secondo relativo ai reati contro la riservatezza informatica avrebbe dovuto tener conto delle modifiche appena apportate dal d.lgs. in materia di frodi e falsificazioni dei mezzi di pagamento diversi dai contanti.

L'ampliamento dell'oggetto del reato e delle condotte sanzionate in assenza di un disegno organico ha quale conseguenza che, in un panorama già complesso, l'individuazione dei rapporti tra le diverse fattispecie è divenuta ardua o quasi impossibile.

Si sono già esaminate le possibili sovrapposizioni tra i reati di frode informatica ex art. 640-*ter* c.p. e indebito uso e falsificazione degli strumenti di pagamento diversi dai contanti ex 493-*ter* c.p.; nonché tra i reati di detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici di cui all'art. 615-*quater* c.p. e il nuovo reato di cui all'art. 493-*quater* c.p. In realtà il potenziale conflitto tra le

[62] Sulla rilevanza penale del *phishing* sia consentito rinviare, anche per i necessari riferimenti bibliografici, a CRESCIOLI, *Le diverse fasi dei* phishing attacks*: le fattispecie vigenti e i problemi applicativi in prospettiva comparata tra Italia e Germania*, in *Ind. pen.*, 2021, 3, 799 ss.

[63] Al *Considerando* n. 6.

[64] V. il *Considerando* n. 15 della direttiva 2019/713/UE.

diverse norme è molto più ampio e finisce per coinvolgere la quasi totalità delle fattispecie esaminate e oggetto di una o dell'altra modifica legislativa.
Per riuscire a carpire da remoto i dati personali o le credenziali altrui, allo scopo di effettuare un accesso abusivo finalizzato ad una frode informatica, qualora non sia la vittima stessa a fornirle al criminale, perché tratta in inganno dai messaggi di *phishing*, è necessaria la previa installazione di un *malware* nel computer della vittima, che intercetti i dati in entrata o in uscita e dunque anche le sue *password*. Tale condotta, oltre che alla frode informatica ed eventualmente all'accesso abusivo ad un sistema informatico o telematico protetto da misure di sicurezza e al reato di cui all'art. 615-*quater* c.p., è astrattamente riconducibile anche al reato di cui all'art. 617-*quater* c.p., che sanziona, come si è visto in precedenza (v. *retro* par. 5.1) l'intercettazione, l'impedimento o l'interruzione illecita di comunicazioni informatiche o telematiche.
La norma in esame non descrive quale debba essere il contenuto della comunicazione, né si richiede che essa avvenga tra persone: per cui oggetto dell'intercettazione possono essere anche informazioni, notizie e dati, dunque anche i codici alfanumerici di accesso utenti[65]. La Cassazione ha ritenuto applicabile il reato di cui all'art. 617-*quater* c.p. anche all'utilizzo di carte di credito clonate[66].
Al fine di intercettare le comunicazioni del sistema informatico si rende anche necessario installare apparecchiature volte a intercettare i dati trasmessi, per cui si potrebbe astrattamente configurare anche l'ulteriore e diverso reato di cui all'art. 617-*quinquies* c.p. Seppure sia innegabile che le condotte sanzionate dalle diverse fattispecie siano in qualche misura eterogenee e che in alcuni casi i reati si consumano in momenti differenti, dato che l'intercettazione, l'installazione del *malware*, l'apprensione di *password* altrui,

[65] Così Cass., Sez. II, 9 novembre 2007, n. 45207 secondo cui «*Integra la condotta di "intercettazione", rilevante ai sensi dell'art. 617 quater c.p., la condotta di colui che utilizza apparecchiature idonee a copiare degli i codici alfanumerici di accesso utenti, mediante applicazione ai terminali automatici delle banche. La digitazione del codice di accesso costituisce, invero, la prima comunicazione dell'utente con il sistema informatico, con la conseguenza che la copiatura di detti codici rientra nel concetto di intercettazione di comunicazioni telematiche preso in considerazione dalla citata disposizione normativa*»; nello stesso senso anche Cass., Sez. V, 30 gennaio 2007, n. 3252.
[66] Cass., Sez. V, 14 ottobre 2003, n. 44362.

ecc. vengono effettuate proprio allo scopo di accedere abusivamente al sistema informatico altrui o alterare la *App* di accesso ai servizi bancari, ecc., non si può trascurare come anche così i reati siano tra loro in rapporto di stretta consequenzialità. Pertanto, le fattispecie potenzialmente applicabili al singolo attacco informatico sono davvero numerose.

In molti casi vi è una vera e propria progressione criminosa, ma è difficile concludere per l'applicabilità di una sola norma. Questo perché la giurisprudenza prevalente delle Sezioni Unite supporta un criterio monistico, basato esclusivamente sul rapporto strutturale tra norme ed esclude così l'utilizzabilità di criteri diversi da quello legislativo di specialità[67]. Ma in questi casi è difficile individuare un rapporto di specialità, sia per la diversità strutturale delle norme, sia perché molte fattispecie si consumano in tempi fisiologicamente differenti. Inoltre, nonostante sia vero che, come sottolineato recentemente anche dalle Sezioni Unite[68], il principio di specialità non può finire per abrogare la disciplina del reato complesso, nelle ipotesi in esame è assai arduo individuare quale tra i tanti sia il reato complesso che assorbe in sé il disvalore di tutte le fattispecie. Questo anche perché, a seguito di entrambe le novelle legislative qui esaminate, sono state aumentate le pene edittali: perciò, a parte i reati di cui agli artt. 615-*quater* e 493-*quater* c.p. che effettivamente hanno un trattamento sanzionatorio meno severo, che consente di operare un assorbimento, le altre fattispecie esaminate hanno tutte un trattamento sanzionatorio simile.

Si aggiunga poi che l'art. 617-*quater* c.p. prevede una pena superiore alle fattispecie base di frode informatica e a quella dell'art. 493-*ter* c.p. e dell'art. 615-*ter* c.p., al pari dell'art. 617-*quinquies* c.p., che punisce proprio condotte prodromiche alla realizzazione dell'accesso abusivo al sistema informatico, frode informatica o falsificazione di strumenti di pagamento, ma è proprio perché

[67] Cass., Sez. un., 23 febbraio 2017, n. 20664, con nota di FINOCCHIARO, *Il buio oltre la specialità. Le Sezioni Unite sul concorso tra truffa aggravata e malversazione*, in *www.penalecontemporaneo.it*, 8 maggio 2017, 1 e Cass., Sez. un., 12 settembre 2017, n. 41588, con nota di SERRA, *Le Sezioni Unite e il concorso apparente di norme, tra considerazioni tradizionali e nuovi spunti interpretativi*, in *Dir. pen. cont.*, 2017, 11, 173 ss. In senso conforme anche Cass., Sez. un., 28 ottobre 2010, n. 1963; Cass., Sez. un., 28 ottobre 2010, n. 1235; Cass., Sez. un., 19 aprile 2007, n. 16568; Cass., Sez. un., 20 dicembre 2005, n. 47164; Cass., Sez. un., 9 maggio 2001, n. 23427; Cass., Sez. un., 28 marzo 2001, n. 22902.

[68] Cass., Sez. un., 26 ottobre 2021, n. 38402, in *www.sistemapenale.it*, 3 novembre 2021.

non appare possibile operare alcun assorbimento, per cui non vi è altra soluzione che ritenere che le fattispecie elencate possano tra loro concorrere.
In tale contesto l'art. 81 c.p. assume un ruolo chiave, perché consente di mitigare il trattamento sanzionatorio, che altrimenti sarebbe sproporzionato e, come auspicato da una parte della dottrina[69], in alcuni casi si potrebbe persino operare il c.d. aumento zero.
Al fine di evitare irragionevoli ed ingiustificate duplicazioni sanzionatorie si dovrebbe pertanto procedere ad un profondo e meditato riordino della materia, anche tramite l'abrogazione di qualche fattispecie, mantenendo, però, inalterata la rilevanza penale delle condotte indicate nelle menzionate direttive europee.

7. *Brevi riflessioni conclusive.* Il fatto che il legislatore italiano abbia finalmente emanato i provvedimenti legislativi di attuazione delle due direttive europee sopra menzionate non può che essere accolto con favore. Tuttavia, nonostante l'apprezzabile sforzo, il legislatore italiano, come sopra evidenziato, non ha recepito correttamente le menzionate direttive. In particolare, ha tralasciato del tutto di adottare le misure necessarie in materia di giurisdizione. È dunque estremamente probabile che in futuro vi saranno ulteriori contestazioni da parte della Commissione europea.
Inoltre, non si comprende il motivo per cui l'attuazione di tali direttive è avvenuta con atti legislativi separati. Tale scelta ha accentuato il già presente problema della sovrapposizione delle norme penali, per cui uno stesso fatto può ricondursi contemporaneamente ed indifferentemente a più incriminazioni tra loro diversissime. Infatti, se da un lato il legislatore ha giustamente ampliato in alcuni casi l'oggetto del reato, nonché il novero delle condotte punibili, adattando le fattispecie al mutato contesto tecnologico e sociale, dall'altro non si è minimamente preoccupato di garantire un certo coordinamento tra le diverse norme. Tuttavia, il ripetersi di casi di tipicità doppia e magari anche plurima di un fatto, costituisce senz'altro una compromissione dell'esigenza di tassatività. Ciò perché quando la formulazione legislativa è ambigua e indeterminata circa la definizione giuridico-penale di un fatto;

[69] SOTIS, *Il "concorso materiale apparente": confine tra artt. 15 e 81 c.p.*, in *Giur. it.*, 2020, 1, 193.

quindi, in definitiva circa il tipo e il *quantum* della sanzione da applicare al fatto medesimo, si conferisce al giudice uno spazio di discrezionalità incompatibile col dettato dell'art. 25 co. 2 Cost.
È quindi evidente che i menzionati interventi legislativi non sono affatto sufficienti, ma è invece necessario un profondo riordino della materia, anche tramite l'abrogazione di qualche fattispecie al fine di evitare irragionevoli ed ingiustificate duplicazioni sanzionatorie. Sempre però mantenendo inalterata la rilevanza penale delle condotte indicate nelle direttive europee.