NOVITÀ SOVRANAZIONALI
SUPRANATIONAL NEWS

di *Elena Zanetti*

UNA NUOVA DIRETTIVA EUROPEA IN TEMA DI LOTTA CONTRO LE FRODI E LE FALSIFICAZIONI DI MEZZI DI PAGAMENTO DIVERSI DAI CONTANTI

Con la direttiva (UE) 2019/713 del Parlamento e del Consiglio del 17 aprile 2019 (pubblicata in G.U.U.E., 10 maggio 2019, L 123) l'Unione europea interviene nel settore nevralgico dei reati concernenti i mezzi di pagamento alternativi ai contanti, sostituendo la precedente Decisione quadro 2001/413/GAI del Consiglio del 28 maggio 2001 (in G.U.U.E., 2 giugno 2001, L 149). Valutata l'entità delle modifiche e delle integrazioni necessarie ad aggiornare quest'ultima, si è, infatti, ritenuto più opportuno sostituirla integralmente con un nuovo testo, adottato in base al principio di sussidiarietà enunciato nell'art. 5 del Trattato sull'Unione europea. Per gli Stati membri vincolati dalla nuova direttiva i riferimenti alla Decisione quadro 2001/413/GAI devono intendersi, quindi, riferiti alla direttiva in esame (art. 19).

Come si afferma nel preambolo (considerandi nn. 1-41), l'aggiornamento e l'integrazione del quadro normativo di riferimento sono stati sollecitati – sotto diversi profili – dalla progressiva diffusione e dalla costante evoluzione degli strumenti di pagamento diversi dai contanti, incentivate dalla crescita esponenziale dell'economia digitale (considerando n. 6). Le nuove tecnologie di pagamento, infatti, «*da un lato creano nuove opportunità per i consumatori e le imprese, ma dall'altro aumentano anche le opportunità di frode*». Le frodi e le falsificazioni di tali innovative forme di pagamento costituiscono, in primo luogo, una minaccia alla sicurezza, poiché «*rappresentano fonti di entrate per la criminalità organizzata*», rendendo possibili altre attività criminose quali il terrorismo, il traffico di droga e la tratta di esseri umani (considerando n. 1). Esse configurano, inoltre, «*un ostacolo al mercato unico digitale, intaccando la fiducia dei consumatori e causando una perdita economica diretta*» (considerando n. 2).

Anche in ragione dell'accentuata connotazione digitale dei nuovi mezzi di pagamento, i reati di frode e di falsificazione ad essi relativi denotano una rilevante dimensione transfrontaliera, «*che sottolinea la necessità di un'azione di ravvicinamento del diritto penale*» (considerando n. 5), poiché la presenza negli ordinamenti nazionali degli Stati membri di lacune e di differenze considerevoli sul punto «*può ostacolare la prevenzione, l'individuazione e il perseguimento di questi tipi di reato e di altre forme gravi di criminalità organizzata ad essi connesse e da esse facilitate*», oltre a rendere *più difficile la cooperazione di polizia e la cooperazione giudiziaria, e quindi meno efficaci, con conseguenze negative sul piano della sicurezza*» (considerando n. 3).

Il considerando n. 40 provvede a focalizzare gli obiettivi della direttiva. In particolare, essa intende assoggettare «*a sanzioni penali effettive, proporzionate e dissuasive*» i reati di frode e di falsificazione dei mezzi di pagamento di natura digitale, nonché «*migliorare e incoraggiare la cooperazione transfrontaliera tra le autorità competenti e tra le persone fisiche e giuridiche e le autorità competenti*».

Gli Stati membri dovranno recepire la direttiva (UE) 2019/713, entrata in vigore – ai sensi dell'art. 22 – il ventesimo giorno successivo alla pubblicazione sulla Gazzetta Ufficiale, come disposto dall'art. 19, entro il 31 maggio 2021. Non sono vincolati dalla direttiva, né sono soggetti alla sua applicazione il Regno Unito e l'Irlanda – a norma degli artt. 1 e 2 del protocollo n. 21 allegato al TUE e al TFUE – oltre alla Danimarca – a norma degli artt. 1 e 2 del protocollo n. 22 allegato al TUE e al TFUE.

Il testo è formato da ventidue articoli, ripartiti nei titoli di seguito elencati: Titolo I – *Oggetto e definizioni* (artt. 1-2); Titolo II – *Reati* (artt. 3-11); Titolo III – *Giurisdizione e indagini* (artt. 12-13); Titolo IV – *Scambio di informazioni e comunicazione dei reati* (artt. 14-22).

Disposizioni generali (oggetto e definizioni)

Come si enuncia nell'art. 1, la direttiva contiene "norme minime" «*relative alla definizione dei reati e delle sanzioni nelle materie di frode e di falsificazione di mezzi di pagamento diversi dai contanti*». *Tale previsione implica che agli Stati membri sia riconosciuta, di conseguenza, la facoltà di «adottare o mantenere norme di diritto penale più rigorose»* rispetto alle ipotesi di reato *de quibus*, «*compresa una più ampia definizione dei reati*» stessi (considerando n. 18). Rimarcando la distanza rispetto al contenuto della Decisione quadro 2001/413/GAI, completano l'oggetto della direttiva «*la prevenzione di detti reati nonché la prestazione di assistenza e il sostegno alle vittime*» (art. 1).

Considerato l'elevato tecnicismo della materia *de qua*, la possibilità per gli Stati di esprimere un approccio coerente nell'applicazione della direttiva e di facilitare lo scambio di informazioni e la cooperazione tra le autorità competenti è subordinata alla disponibilità di definizioni comuni (considerando n. 8). In tal senso, l'art. 2 fornisce le definizioni di taluni termini "chiave" (lett. *a-g*), in parte formulandole in via autonoma, in parte richiamando quelle contenute in altri testi normativi.

In particolare, ai fini della direttiva, con l'espressione «*strumento di pagamento diverso dai contanti*» *si intende «un dispositivo, oggetto o record protetto immateriale o materiale, o una loro combinazione, diverso dalla moneta a corso legale, che, da solo o unitamente a una procedura o a una serie di procedure, permette al titolare o all'utente di trasferire denaro o valore monetario, anche attraverso mezzi di scambio digitali»* (lett. *a*). Si specifica poi che per «*dispositivo, oggetto o record protetto*» deve intendersi «*un dispositivo, oggetto o record protetto contro le imitazioni o l'utilizzazione fraudolenta, per esempio mediante disegno, codice o firma*» (lett. *b*). La nozione di «*valuta virtuale*» va, invece, intesa alla stregua di «*una rappresentazione di valore digitale che non è emessa e garantita da una banca centrale o da un ente pubblico, non è legata necessariamente a una valuta legalmente istituita e non possiede lo status giuridico di valuta o denaro, ma è accettata da persone fisiche o giuridiche come mezzo di scambio, e che può essere trasferita, memorizzata e scambiata elettronicamente*» (lett. *d*).

Chiarisce, infine, l'art. 2 che «*persona giuridica*» è «*qualsiasi entità che abbia personalità giuridica in forza del diritto applicabile, ad eccezione degli Stati o di altri organismi pubblici nell'esercizio dei pubblici poteri e delle organizzazioni internazionali pubbliche*» (lett. *g*).

Sono, invece, definite *per relationem*, le nozioni di «*mezzo di scambio digitale*», da intendersi come qualsiasi moneta elettronica «*definita dall'articolo 2, punto 2 della direttiva 2009/110/CE*» concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica e «*la valuta virtuale*» (lett. *c*); e quelle di «*sistema di informazione*» e di «*dati informatici*», entrambe attinte dall'art. 2 della direttiva 2013/40/UE (lett. *e* e lett. *f*).

Le fattispecie incriminatrici

Se la Decisione quadro 2001/413/GAI si limitava ad elencare – nell'art. 2 – attraverso il mero *nomen iuris* alcune ipotesi di reato (furto e appropriazione indebita; contraffazione e falsificazione; ricezione, ottenimento, trasporto, vendita o cessione, detenzione; utilizzazione fraudolenta) commesse «*con strumenti di pagamento*» diversi dalla moneta a corso legale, che gli Stati membri avrebbero dovuto contemplare nei rispettivi ordinamenti nazionali, la direttiva in commento intende fornire una «*impostazione comune*» per quanto attiene agli elementi costitutivi delle diverse condotte illecite considerate.

Va precisato, inoltre, che la direttiva non prevede figure di reato di nuovo tipo, ma "adatta" al settore dei mezzi di pagamento diversi dai contanti, grazie ad un minuzioso lavoro di elaborazione, talune forme "classiche" di reato «*definite dal diritto nazionale già prima dell'era digitale*» (considerando n. 15). Rispetto a queste ultime, le fattispecie menzionate nel titolo II rappresentano – per così dire – le corrispondenti tipologie di condotte in ambito digitale.

In tal senso, il reato di "utilizzazione fraudolenta" – come definito dall'art. 3 – può essere perpetrato alternativamente o mediante uno strumento di pagamento diverso dai contanti «*rubato o altrimenti illecitamente ottenuto ovvero oggetto di illecita appropriazione*» (lett. *a*), o mediante uno strumento «*contraffatto o falsificato*» (lett. *b*). In aggiunta a questa prima ipotesi di reato, gli artt. 4 e 5 enumerano varie ulteriori fattispecie connesse all'utilizzo fraudolento di strumenti di pagamento diversi dai contanti, rispettivamente, di tipo materiale e di tipo immateriale.

Nel primo gruppo rientrano le condotte di furto o di altra illecita appropriazione; di contraffazione o di falsificazione fraudolenta; di possesso di uno strumento materiale di pagamento «*rubato o altrimenti ottenuto mediante illecita appropriazione, o contraffatto o falsificato a fini di utilizzazione fraudolenta*»; nonché l'atto di procurare per sé o per altri, compresi la ricezione, l'appropriazione, l'acquisto, il trasferimento,

l'importazione, l'esportazione, la vendita, il trasporto e la distribuzione di uno strumento materiale di pagamento «*rubato, contraffatto o falsificato a fini di utilizzazione fraudolenta*» (art. 4).

Nel secondo sono, invece, annoverati i casi di ottenimento illecito e di appropriazione indebita; di contraffazione e di falsificazione fraudolenta; di detenzione di uno strumento immateriale di pagamento «*ottenuto illecitamente, contraffatto o falsificato a fini di utilizzazione fraudolenta*»; l'atto di procurare per sé o per altri, compresi la vendita, il trasferimento e la distribuzione, o la messa a disposizione di uno strumento immateriale di pagamento «*ottenuto illecitamente, contraffatto o falsificato a fini di utilizzazione fraudolenta*» (art. 5).

Integra, invece, la diversa ipotesi di "frode connessa ai sistemi di informazione" 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*», commesso intenzionalmente al fine di ostacolare, senza diritto, «*il funzionamento di un sistema di informazione o interferendo con esso*» o «*introducendo, alterando, cancellando, trasmettendo o sopprimendo, senza diritto, dati informatici*» (art. 6).

Oltre ad adottare le misure necessarie affinché nei rispettivi ordinamenti siano previste e punibili le fattispecie contemplate dagli artt. 3-6, gli Stati membri dovranno provvedere in tal senso – in forza dell'art. 7 – anche riguardo ai mezzi utilizzati per commettere quei reati, quali in particolare «*la fabbricazione, l'ottenimento per sé o per altro, inclusi l'importazione, l'esportazione, la vendita, il trasporto o la distribuzione, o la messa a disposizione di un dispositivo o di uno strumento, di dati informatici o di altri mezzi principalmente progettati o specificamente adattati*» allo scopo di compiere uno dei reati «*di cui all'art. 4, lettere a) e b), all'articolo 5, lettere a) e b) o all'articolo 6, almeno se commessi con l'intenzione di utilizzare tali mezzi*».

Si chiarisce poi nell'art. 8, che i reati contemplati nel titolo II dovranno essere punibili da parte dei sistemi nazionali dei singoli Stati anche in forma di istigazione, favoreggiamento, concorso, ed, in ossequio alle previsioni di dettaglio contenute nel par. 2, anche di tentativo.

Di tutti i reati *de quibus* potranno, inoltre, essere ritenute responsabili le persone giuridiche, in presenza dei requisiti e nei limiti stabiliti dall'art. 10. A tal fine, è richiesto che il reato sia commesso a vantaggio della persona giuridica «*da qualsiasi persona che agisca a titolo individuale o in quanto membro di un organismo*» interno ad essa o che occupi in essa «*una posizione preminente*» in forza di un potere di rappresentanza, o in quanto dotata dell'autorità di adottare decisioni per conto della persona giuridica o di esercitare un controllo in seno ad essa (par. 1). Del pari, la responsabilità delle persone giuridiche potrà configurarsi anche qualora l'omessa sorveglianza o il mancato controllo da parte di uno dei soggetti indicati nel par. 1 abbia reso possibile la commissione di uno dei reati di cui agli artt. 3 – 8 a vantaggio della persona giuridica stessa (par. 2).

Le sanzioni applicabili

L'obiettivo di punire i reati *de quibus* con pene e sanzioni «*effettive, proporzionate e dissuasive*» è perseguito dalla direttiva, in primo luogo, mediante la previsione di sanzioni differenziate per le persone fisiche (art. 9) e per le persone giuridiche (art. 11).

In merito alle prime, l'art. 9, oltre a richiamare, in via generale, gli Stati membri ad adottare sanzioni effettive per tutti i reati contemplati dal titolo II, individua limiti edittali massimi di pena detentiva cui gli ordinamenti nazionali dovranno uniformarsi rispetto a singole ipotesi di reato. A seconda della fattispecie considerata vengono così individuate le seguenti quattro soglie: pena massima non inferiore a un anno per i reati di cui all'art. 4, lettere *c*) e *d*) e di cui all'art. 5, lettere *c*) e *d*); pena massima non inferiore a due anni per i reati di utilizzazione fraudolenta di cui all'art. 3, per i reati di cui all'art. 4, lett. *a*) e *b*), e all'art. 5, lett. *a*) e *b*), nonché all'art. 7; pena massima non inferiore a tre anni per i reati di frode connessa ai sistemi di informazione di cui all'art. 6; pena massima non inferiore a cinque anni per i reati di cui agli artt. da 3 a 6, qualora siano commessi nell'ambito di un'organizzazione criminale, riconducibile alla Decisione quadro 2008/841/GAI relativa alla lotta contro la criminalità organizzata, indipendentemente dalla sanzione ivi prevista.

Ferma restando l'introduzione di tali soglie, è opportuno ribadire come la direttiva lasci comunque impregiudicate l'individualizzazione del trattamento sanzionatorio, nonché l'applicazione delle sanzioni e l'esecuzione delle sentenze nel rispetto «*delle circostanze del caso specifico e delle norme generali di diritto penale nazionale*» (considerando n. 17).

Riguardo alle seconde, si demanda agli Stati membri la possibilità di scelta tra sanzioni di natura diversa. Nei confronti delle persone giuridiche riconosciute responsabili di reato ai sensi dell'art. 10, po-

tranno essere, infatti, adottate sanzioni pecuniarie penali e sanzioni non penali. In quest'ultima categoria l'art. 11 include, a titolo esemplificativo, l'esclusione dal godimento di un beneficio o di un aiuto pubblico; l'esclusione temporanea dall'accesso ai finanziamenti pubblici, comprese procedure di gara, sovvenzioni e concessioni; l'interdizione temporanea o permanente di esercitare un'attività commerciale; l'assoggettamento a sorveglianza giudiziaria; provvedimenti giudiziari di scioglimento; la chiusura temporanea o permanente dei locali usati per commettere il reato.

Giurisdizione

Quanto alle regole in base alle quali affermare la giurisdizione degli Stati membri sui reati previsti dal titolo II della direttiva, l'art. 12 – attenendosi al generale principio di efficacia operante in materia e uniformandosi agli usuali criteri attributivi – individua nel sistema giudiziario del Paese in cui il reato è stato commesso quello più idoneo a trattarlo (considerando n. 20). Ciascuno Stato membro stabilirà, dunque, la propria giurisdizione sui reati commessi, anche solo in parte, sul suo territorio e su quelli commessi da un suo cittadino. A corredo di tale statuizione, si chiarisce che un reato è «*commesso in tutto o in parte sul territorio di uno Stato membro*» quando l'autore lo compie «*mentre era fisicamente presente in quel territorio e, indipendentemente dal fatto che il sistema di informazione con cui è stato commesso il reato si trovasse o meno nel suo territorio*» (par. 2).

Il par. 3 dell'art. 12 non manca poi di prevedere criteri attribuivi supplementari, in base ai quali agli Stati membri è consentito estendere la propria giurisdizione anche su reati commessi al di fuori del territorio nazionale. Tale eventualità si prospetta, in via alternativa, allorché l'autore del reato risieda abitualmente nel territorio dello Stato; il reato sia commesso a vantaggio di una persona giuridica che ha sede sul territorio dello Stato; e qualora il reato sia stato commesso contro un cittadino dello Stato o contro una persona che risieda abitualmente sul suo territorio.

In caso di conflitti di giurisdizione – richiamando gli obblighi rispettivamente derivanti dalla Decisione quadro 2009/948/GAI del 30 novembre 2009 sulla prevenzione e la risoluzione dei conflitti relativi all'esercizio della giurisdizione nei procedimenti speciali e la Decisione quadro 2002/187/GAI del 28 febbraio 2002 che istituisce l'Eurojust per rafforzare la lotta contro le forme gravi di criminalità – le autorità competenti degli Stati membri interessati sono incoraggiate ad avviare consultazioni dirette anche avvalendosi dell'assistenza dell'Agenzia dell'Unione europea per la cooperazione giudiziaria penale (considerando n. 21).

Indagini e cooperazione

La delicatezza e la complessità delle indagini sulle frodi e le falsificazioni dei mezzi di pagamento diversi dai contanti richiedono che le autorità competenti degli Stati membri possano disporre di strumenti «*efficaci e proporzionati*». A tal fine l'art. 13 dispone che «*le persone, le unità o i servizi incaricati delle indagini o dell'azione penale*» abbiano accesso agli strumenti utilizzati nel contrasto alla criminalità organizzata o ad altre forme gravi di criminalità.

Di pari importanza per un'efficace azione di contrasto da parte delle autorità competenti è la possibilità di «*accedere tempestivamente alle informazioni utili per svolgere le indagini e perseguire i reati*» (considerando n. 22). Su questo fronte la direttiva considera tre diverse situazioni, distinguendo tra circolazione delle informazioni (art. 13, par. 2), scambio di informazioni (art. 14) e comunicazione dei reati (art. 15).

Per favorire la circolazione delle informazioni sui reati di cui agli articoli 3 – 8 gli Stati membri adottano le misure necessarie per consentire che tali informazioni giungano «*senza indugio alle autorità che indagano o perseguono tali reati*», le quali dovrebbero essere altresì autorizzate a «*cooperare con altre autorità nazionali nello Stato membro e con le loro controparti in altri Stati membri*» (considerando n. 23).

Sul versante dello scambio di informazioni tra le autorità nazionali di contrasto, la direttiva valorizza il ruolo dei "punti di contatto operativi" istituiti dalla Decisione quadro 2001/413/GAI (art. 12). L'art. 14 prevede che gli Stati membri predispongano a tal fine «*un punto di contatto operativo nazionale disponibile ventiquattr'ore su ventiquattro, sette giorni su sette*» (art. 14, par. 1), dotandosi di procedure che consentano di trattare in modo tempestivo le richieste urgenti di assistenza – anche provenienti dalla rete – e di rispondere entro otto ore dalla presentazione. I punti di contatto dovrebbero fornire «*un'assistenza concreta, ad esempio facilitando lo scambio di informazioni pertinenti*», comprese consulenze tecniche e informazioni giuridiche (considerando n. 26).

Notizie aggiornate sul punto di contatto nazionale devono essere comunicate, in conformità alle rispettive attribuzioni, alla Commissione, ad Europol e ad Eurojust (art. 14, par. 2).

Tenuto conto che la comunicazione dei reati alle autorità competenti rappresenta spesso «*il punto di partenza di indagini giudiziarie*» (considerando n. 27), gli Stati membri sono sollecitati a rendere disponibili "canali adeguati" per agevolare tale comunicazione alle autorità nazionali di contrasto e alle altre autorità competenti (art. 15, par. 1). Per perseguire tale finalità, le istituzioni finanziarie e le altre persone giuridiche che operano sul territorio degli Stati membri vanno incentivate, attraverso l'adozione di misure *ad hoc*, a riferire «*senza indebito ritardo i sospetti di frode*» (art. 15, par. 2).

Gli Stati membri sono, inoltre, incoraggiati ad assicurare «*un'applicazione efficace degli strumenti di riconoscimento reciproco e di mutua assistenza giudiziaria riguardo ai reati coperti dalla presente direttiva*» (considerando n. 29). Lo sviluppo di efficaci rapporti di cooperazione risulta, infatti, funzionale a perseguire in modo proficuo gli obiettivi della direttiva stessa dal momento che tali reati hanno sovente carattere transfrontaliero.

Alle disposizioni in materia di indagini si collegano quelle in tema di prevenzione contemplate nell'art. 17, che individua una serie di "azioni adeguate" da realizzare anche attraverso internet – quali campagne di informazione e di sensibilizzazione e programmi di ricerca e di istruzione – volte a ridurre l'incidenza delle frodi, sensibilizzare il pubblico e ridurre il rischio di incorrere in quel tipo di reato.

Assistenza e sostegno alle vittime

Le frodi e le falsificazioni di mezzi di pagamento alternativi ai contanti possono causare gravi conseguenze non solo di natura economica – si pensi, ad esempio, al furto di identità – in danno di chi ne è vittima. Sovente, ad aggravare ulteriormente tali ricadute contribuisce poi il fattore tempo, innescando reati connessi che amplificano in modo esponenziale gli effetti dannosi derivanti dai reati *de quibus* (considerando n. 31).

Per rispondere alla specificità di tali possibili scenari la direttiva (UE) 2019/713 introduce forme di assistenza, di natura prevalentemente informativa, aggiuntive rispetto a quelle che già derivano dalla Direttiva 2012/29/UE del 25 ottobre 2012 che istituisce norme minime in materia di diritti, assistenza e protezione delle vittime di reato.

Alle persone fisiche e giuridiche che abbiano subito un danno derivante dai reati previsti dal titolo II della direttiva in esame, commessi mediante l'uso fraudolento di dati personali, vanno comunicati «*dati informazioni e consigli specifici*» su come proteggersi dalle conseguenze negative che da essi derivano, quale il danno alla reputazione; nonché un «*elenco delle istituzioni che si occupano specificamente di diversi aspetti del reato connesso all'identità e del sostegno delle vittime*» (art. 16, par. 1). L'accesso delle vittime alle forme di assistenza e di sostegno può essere semplificato anche mediante l'istituzione di «*strumenti nazionali unici di informazione online*» (art. 16, par. 2).

In seguito al primo contatto con l'autorità giudiziaria, alla vittima sono, inoltre, dovute – ai sensi del diritto nazionale – le informazioni concernenti le procedure per presentare una denuncia relativa al reato e il ruolo della vittima in tali procedure;

Disposizioni finali

Al più tardi entro il 31 agosto 2019 la Commissione è chiamata ad istituire un "programma dettagliato" di monitoraggio degli esiti, dei risultati e degli effetti della direttiva. Nel programma devono essere messi a punto, tra l'altro, i mezzi da utilizzare e la periodicità della raccolta dei dati (art. 18).

Ulteriori scadenze sono previste dall'art. 21 per la presentazione di relazioni e di valutazioni da parte della Commissione. Entro il 31 maggio 2023 andrà presentata al Parlamento e al Consiglio la relazione che valuta in quale misura gli Stati membri si siano conformati alla direttiva. Entro il 31 maggio 2026 sarà presentata la relazione relativa all'impatto della direttiva stessa.

Da segnalare, infine, che il testo delle disposizioni interne adottate degli Stati membri per conformarsi alla direttiva deve essere comunicato alla Commissione (art. 20, par. 2).