Consiglio
dell'Unione europea

Bruxelles, 11 luglio 2023
(OR. en)

11761/23

CYBER 184
DROIPEN 107
IA 180
JAI 998
MI 607
TELECOM 229

NOTA DI TRASMISSIONE

Origine:	Segretaria generale della Commissione europea, firmato da Martine DEPREZ, direttrice
Data:	10 luglio 2023
Destinatario:	Thérèse BLANCHET, segretaria generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2023) 363 final
Oggetto:	RELAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO che valuta in quale misura gli Stati membri abbiano adottato le misure necessarie per conformarsi alla direttiva (UE) 2019/713 relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti e che sostituisce la decisione quadro 2001/413/GAI del Consiglio

Si trasmette in allegato, per le delegazioni, il documento COM(2023) 363 final.

All.: COM(2023) 363 final

COMMISSIONE
EUROPEA

Bruxelles, 10.7.2023
COM(2023) 363 final

RELAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO E AL CONSIGLIO

che valuta in quale misura gli Stati membri abbiano adottato le misure necessarie per conformarsi alla direttiva (UE) 2019/713 relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti e che sostituisce la decisione quadro 2001/413/GAI del Consiglio

1. INTRODUZIONE

Le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti, quali le carte di credito o le carte di pagamento, rappresentano fonti di entrate per la criminalità organizzata e rendono possibili altre attività criminali come il terrorismo, il traffico di droga e la tratta di esseri umani. Tali reati causano perdite ingenti: nel 2019 il valore totale delle operazioni fraudolente effettuate con carte emesse all'interno dell'area unica dei pagamenti in euro (SEPA) è stato pari a 1,87 miliardi di EUR[1]. La stragrande maggioranza delle operazioni fraudolente riguarda le frodi "carta non presente" (*card-not-present*, CNP): nel 2019 l'80 % del valore delle frodi relative alle carte di pagamento è derivato da operazioni CNP, ossia da pagamenti tramite Internet, posta o telefono[2]. Nel 2019 le frodi CNP hanno causato perdite pari a 1,50 miliardi di EUR, in aumento del 4,3 % rispetto all'anno precedente[3].

Esiste una chiara dimensione transfrontaliera: nel 2019 più della metà del valore totale delle frodi ha riguardato operazioni transfrontaliere all'interno della SEPA. Dal punto di vista geografico, nel 2019 le operazioni nazionali hanno rappresentato l'89 % del valore di tutte le operazioni tramite carta, ma soltanto il 35 % delle operazioni fraudolente. In termini di valore, le operazioni transfrontaliere all'interno della SEPA hanno rappresentato il 9 % di tutte le operazioni tramite carta, ma il 51 % delle frodi comunicate[4].

Per contrastare questi reati in maniera efficace, gli Stati membri devono definire insieme quali atti debbano essere considerati frodi e falsificazioni di mezzi di pagamento diversi dai contanti. Devono anche ravvicinare i livelli di sanzioni e disporre dei mezzi operativi per la comunicazione dei reati e lo scambio di informazioni fra le autorità. Di conseguenza il 17 aprile 2019 il Parlamento europeo e il Consiglio hanno adottato la direttiva (UE) 2019/713 ("direttiva") relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti e che sostituisce la decisione quadro 2001/413/GAI del Consiglio[5]. La presente relazione risponde all'obbligo di cui all'articolo 21 della direttiva.

1.1. Obiettivi e ambito di applicazione della direttiva

La direttiva mira a ravvicinare il diritto penale degli Stati membri[6] nel settore delle frodi e delle falsificazioni di mezzi di pagamento diversi dai contanti e migliorare la cooperazione fra le autorità competenti. In quest'ottica la direttiva stabilisce norme minime relative alla definizione dei reati e delle sanzioni. L'ambito di applicazione della direttiva è vasto e, come indicato all'articolo 2, lettera a), comprende qualsiasi "dispositivo, oggetto o record protetto immateriale o materiale, o una loro combinazione, diverso dalla moneta a corso legale, che,

---

[1] Banca centrale europea, *Seventh report on card fraud* (Settima relazione sulle frodi con carte di pagamento), disponibile all'indirizzo: https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202110~cac4c418e8.en.html

[2] Ibidem.

[3] Ibidem.

[4] Ibidem.

[5] https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv%3AOJ.L_.2019.123.01.0018.01.ITA.

[6] Nel prosieguo, salvo diversa ed esplicita indicazione, per "Stati membri" o "tutti gli Stati membri" si intendono gli Stati membri vincolati dalla direttiva, cioè tutti gli Stati membri dell'UE tranne la Danimarca e l'Irlanda, che non hanno partecipato all'adozione della direttiva rispettivamente in conformità del protocollo sulla posizione della Danimarca allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea (TFUE), e del protocollo n. 21 sulla posizione del Regno Unito e dell'Irlanda.

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"[7]. Ad esempio, in tale definizione rientrerebbe un'applicazione per pagamenti tramite dispositivi mobili insieme alla relativa procedura di autorizzazione (ad esempio un PIN). La definizione comprende anche le valute virtuali di cui all'articolo 2, lettera d), e all'articolo 6.

La direttiva definisce alcuni reati specifici, vale a dire:

- utilizzazione fraudolenta di strumenti di pagamento diversi dai contanti (articolo 3);
- reati connessi all'utilizzazione fraudolenta di strumenti di pagamento materiali diversi dai contanti (articolo 4);
- reati connessi all'utilizzazione fraudolenta di strumenti di pagamento immateriali diversi dai contanti (articolo 5);
- frode connessa ai sistemi di informazione (articolo 6);
- fornitura illecita di mezzi utilizzati per commettere i suddetti reati (articolo 7).

Inoltre la direttiva **estende la responsabilità penale** all'istigazione, al favoreggiamento e al concorso, da parte di persone fisiche e/o giuridiche, in relazione ai suddetti reati e al tentativo di commetterli (articolo 8).

Il livello minimo delle **sanzioni** massime da infliggere per i reati previsti dalla direttiva è stabilito all'articolo 9.

Gli articoli successivi stabiliscono condizioni minime relative alla **responsabilità delle persone giuridiche** (articolo 10) e alle sanzioni, che comprendono sanzioni pecuniarie penali o non penali, e forniscono esempi di altre sanzioni che possono essere applicate nei loro confronti (articolo 11).

L'articolo 12 è inteso a garantire siano perseguiti gli autori dei reati di cui agli articoli da 3 a 8 della direttiva. Uno Stato membro deve stabilire la propria **giurisdizione** se a) il reato è commesso, anche solo in parte, sul suo territorio e/o b) l'autore del reato è un suo cittadino. In altri termini, l'articolo 12, paragrafo 1, lettera a), della direttiva stabilisce il principio di territorialità, mentre dall'articolo 12, paragrafo 1, lettera b), della medesima deriva il principio della competenza determinata dalla cittadinanza del soggetto.

L'articolo 13, paragrafo 1, della direttiva stabilisce che le persone, le unità o i servizi incaricati delle indagini o dell'azione penale per i reati di cui agli articoli da 3 a 8 dovrebbero disporre di **strumenti di indagine** efficaci e proporzionati. Conformemente all'articolo 13, paragrafo 2, della direttiva, le informazioni relative ai reati di cui agli articoli da 3 a 8 dovrebbero pervenire senza indugio alle autorità che indagano o perseguono tali reati.

Per quanto riguarda lo scambio di informazioni, l'articolo 14 impone agli Stati membri di predisporre **punti di contatto** operativi nazionali disponibili ventiquattr'ore su ventiquattro e sette giorni su sette, che possano rispondere a qualsiasi richiesta urgente proveniente dall'estero entro otto ore.

Inoltre l'articolo 15, paragrafo 1, della direttiva impone agli Stati membri di istituire canali adeguati per **comunicare i reati** di cui agli articoli da 3 a 8 alle autorità pubbliche senza indebito ritardo. In particolare, le istituzioni finanziarie sono invitate a comunicare i sospetti

[7] Salvo diversa indicazione, tutti gli articoli menzionati sono quelli della direttiva.

di frode alle autorità di contrasto e alle autorità giudiziarie (articolo 15, paragrafo 2). La comunicazione è spesso il punto di partenza di indagini giudiziarie (considerando 27).

Infine gli articoli 16 e 17 della direttiva riguardano rispettivamente **l'assistenza e il sostegno alle vittime** e **la prevenzione**.

1.2 Scopo e metodologia della relazione

L'articolo 20 della direttiva impone agli Stati membri di mettere in vigore le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla direttiva entro il 31 maggio 2021 e di comunicarne il testo alla Commissione.

La presente relazione risponde all'obbligo di cui all'articolo 21 della direttiva, che impone alla Commissione di presentare al Parlamento europeo e al Consiglio una relazione che valuta in quale misura gli Stati membri abbiano adottato le misure necessarie per conformarsi alla direttiva. La relazione, la prima ai sensi dell'articolo 21, fornisce una panoramica delle principali misure di recepimento adottate dagli Stati membri.

Il recepimento negli Stati membri ha comportato la raccolta di informazioni sulle disposizioni legislative e amministrative pertinenti, la relativa analisi, l'elaborazione di nuovi atti legislativi o – nella maggior parte dei casi – la modifica di atti esistenti, fino all'adozione e infine alla comunicazione alla Commissione.

Entro il termine stabilito per il recepimento (31 maggio 2021), nove Stati membri avevano comunicato alla Commissione di aver portato a termine il recepimento della direttiva e avevano comunicato le rispettive misure di recepimento. Nel luglio 2021 la Commissione ha avviato procedimenti di infrazione per mancata comunicazione delle misure nazionali di recepimento nei confronti degli altri 16 Stati membri: AT, BE, BG, CY, CZ, EL, ES, HR, IT, LU, LV, MT, PL, PT, RO e SI[8]. Da allora 15 Stati membri hanno notificato le proprie misure di recepimento, mentre al 30 aprile 2023 è ancora in corso un procedimento di infrazione per mancata comunicazione delle misure nazionali di recepimento nei confronti di BG[9].

Nella presente relazione, la descrizione e l'analisi successive si basano sulle informazioni relative alle misure nazionali di recepimento fornite dagli Stati membri entro il 31 gennaio 2023. Le notifiche pervenute dopo tale termine non sono state prese in considerazione. Sono state prese in considerazione tutte le misure comunicate riguardanti la legislazione nazionale, nonché le decisioni giudiziarie e, ove opportuno, le teorie giuridiche comuni. Nel corso dell'analisi la Commissione ha contattato direttamente gli Stati membri, nei casi in cui era opportuno, per ottenere informazioni o chiarimenti supplementari. Tutte le informazioni raccolte sono state prese in considerazione ai fini dell'analisi.

Oltre alle problematiche individuate nella presente relazione, è possibile che vi siano altre difficoltà nel recepimento e altre disposizioni non comunicate alla Commissione o futuri sviluppi legislativi e non legislativi. Pertanto la presente relazione non impedisce alla

[8] Nel presente documento, gli Stati membri sono indicati secondo i codici seguenti: http://publications.europa.eu/code/it/it-5000600.htm.

[9] Per informazioni sulle decisioni della Commissione relative ai procedimenti di infrazione consultare l'indirizzo seguente: http://ec.europa.eu/atwork/applying-eu-law/infringements-proceedings/infringement_decisions/?lang_code=it.

Commissione di valutare ulteriormente alcune disposizioni e di continuare a sostenere gli Stati membri nel recepimento e nell'attuazione della direttiva.

2. Misure di recepimento

2.1 Definizioni giuridiche

L'articolo 2 stabilisce le definizioni dei principali termini utilizzati nella direttiva, vale a dire: strumento di pagamento diverso dai contanti; dispositivo, oggetto o record protetto; mezzo di scambio digitale; valuta virtuale; sistema di informazione; dati informatici; persona giuridica.

Gli Stati membri hanno generalmente recepito le definizioni basandosi su leggi anteriori alla direttiva o adottate dopo la sua entrata in vigore. In alcuni casi, pur non essendovi disposizioni specifiche che stabiliscano le definizioni, i reati sono recepiti mediante disposizioni generali del codice penale aventi un ambito di applicazione più ampio, ad esempio disposizioni relative al furto. Pertanto la mancata comunicazione del recepimento letterale di una definizione non è necessariamente indice di incompletezza o di non conformità.

Inoltre diverse definizioni rinviano a definizioni contenute in altre direttive.

a) Strumenti di pagamento diversi dai contanti

Dalla valutazione è emerso almeno un caso di recepimento incompleto, consistente nel mancato aggiornamento della definizione stabilita dalla decisione quadro 2001/413/GAI del Consiglio. Di conseguenza la definizione si riferisce solo agli strumenti di pagamento materiali e, a differenza di quella contenuta nella direttiva, non comprende un "dispositivo, oggetto o record protetto [...] o una loro combinazione".

b) Dispositivo, oggetto o record protetto

Diversi Stati membri non hanno recepito questa definizione (BG, CZ, EE, ES, FI, HR, LT, NL, PL, PT, RO, SI). Il mancato recepimento non è necessariamente considerato un caso di inosservanza, in quanto in genere il significato è di immediata comprensione o può essere desunto dalla formulazione della definizione di "strumento di pagamento diverso dai contanti". In alcuni paesi il concetto è stato esplicitato nei lavori preparatori.

c) Mezzi di pagamento digitali e valuta virtuale

Queste due definizioni sono al centro della direttiva (UE) 2019/713, il cui obiettivo principale era ovviare al fatto che la decisione quadro 2001/413/GAI non rifletteva più le realtà attuali e non affrontava in misura sufficiente le nuove sfide e i nuovi sviluppi tecnologici, quali le valute virtuali e i pagamenti tramite dispositivi mobili, di cui era necessario tenere conto per garantire una risposta globale al fenomeno e colmare le lacune indesiderate a livello di criminalizzazione.

Il problema principale riscontrato in sede di recepimento riguarda la portata del concetto di valuta virtuale quale definita all'articolo 2, lettera d), della direttiva. Se da un lato il concetto di moneta elettronica è stato definito in tutti gli Stati membri (spesso a seguito del

recepimento della direttiva sulla moneta elettronica[10]), dall'altro non sono sempre chiare la definizione e la portata del concetto di valuta virtuale.

In HU la valuta virtuale è considerata alla stregua di un bene e di un dato elettronico e può essere oggetto di confisca di beni e di sequestro. Analogamente in PL la normativa non definisce la valuta virtuale e vi è un certo grado di incertezza in merito alla possibilità che questa rientri nelle diverse fattispecie di reato pertinenti al recepimento della direttiva, sebbene alcuni autori ritengano che la valuta virtuale possa rientrare nell'ambito di applicazione delle disposizioni del codice penale che disciplinano i reati relativi alle informazioni, ai supporti di dati o ai dati di informazione.

Molti Stati membri hanno recepito le definizioni in questione mediante nel settore finanziario piuttosto che nel diritto penale (AT, BE, BG, CY, CZ, DE, EE, EL, ES, HR, HU, LT, LU, LV, SI). Tuttavia non in tutti i casi è presente un rinvio alle pertinenti disposizioni della normativa nazionale che definiscono i reati. Infine tre Stati membri (IT, MT, RO) hanno recepito entrambe le definizioni nei rispettivi codici penali.

d) Sistema di informazione

L'articolo 2, lettera e), definisce il "sistema di informazione" mediante un rinvio all'articolo 2, lettera a), della direttiva 2013/40/UE. Tutti gli Stati membri hanno recepito la definizione conformemente alla direttiva.

e) Dati informatici

I dati informatici sono definiti all'articolo 2, lettera f), mediante un rinvio all'articolo 2, lettera b), della direttiva 2013/40/UE. Tutti gli Stati membri hanno recepito l'articolo 2, lettera f), conformemente alla direttiva.

f) Persona giuridica

Infine l'articolo 2, lettera g), definisce la nozione di "persona giuridica", che quasi tutti gli Stati membri hanno recepito nelle rispettive legislazioni. L'unica eccezione è la SE, che non definisce la nozione di "persona giuridica". Il termine più affine utilizzato nel testo di recepimento è "impresa", che non è definito in alcun testo giuridico, né tantomeno nella dottrina o nella giurisprudenza.

2.2 Reati specifici

a) Utilizzazione fraudolenta di strumenti di pagamento diversi dai contanti

L'articolo 3, lettera a), della direttiva impone agli Stati membri di adottare le misure necessarie affinché, se commessa intenzionalmente, sia punibile come reato l'utilizzazione fraudolenta di uno strumento di pagamento diverso dai contanti rubato o altrimenti illecitamente ottenuto ovvero oggetto di illecita appropriazione.

25 Stati membri hanno recepito l'articolo 3, lettera a), della direttiva. Di questi 25 paesi, 14 hanno recepito la direttiva mediante una disposizione specifica sull'utilizzazione fraudolenta

[10] Direttiva 2009/110/CE del Parlamento europeo e del Consiglio, del 16 settembre 2009, concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica, che modifica le direttive 2005/60/CE e 2006/48/CE e che abroga la direttiva 2000/46/CE (GU L 267 del 10.10.2009, pag. 7).

di strumenti di pagamento diversi dai contanti (AT, CY, ES, FI, HU, IT, LT, MT, NL, PT, RO, SE, SI, SK). Gli altri Stati membri hanno fatto riferimento a fattispecie di reato più generali, quali la frode e la contraffazione informatica o le frodi relative a mezzi di pagamento non circoscritti agli strumenti di pagamento diversi dai contanti (BE, BG, CZ, DE, EE, EL, FR, HR, LU, LV, PL, SE, SK).

In HR la legge non fa riferimento all'utilizzazione di strumenti di pagamento rubati o altrimenti ottenuti mediante illecita appropriazione, e la disposizione di recepimento si riferisce solo agli strumenti di pagamento elettronici diversi dai contanti.

A norma dell'articolo 3, lettera b), della direttiva, gli Stati membri devono adottare le misure necessarie affinché, se commessa intenzionalmente, sia punibile come reato l'utilizzazione fraudolenta di uno strumento di pagamento diverso dai contanti contraffatto o falsificato.

In linea generale l'articolo 3, lettera b), è stato recepito in maniera completa.

Per recepire la direttiva 15 Stati membri rinviano alle disposizioni nazionali sugli strumenti di pagamento diversi dai contanti (AT, CY, DE, EE, ES, FI, HR, HU, IT, LT, MT, NL, PT, RO, SI), mentre in dieci Stati membri la normativa nazionale di recepimento contempla reati più generali, quali il furto o la frode, o reati connessi agli strumenti di pagamento, ma non specificamente agli strumenti diversi dai contanti (BE, BG, CZ, EL, FR, LU, LV, PL, SE, SK).

b) Reati connessi all'utilizzazione fraudolenta di strumenti di pagamento materiali diversi dai contanti

L'articolo 4 della direttiva impone agli Stati membri di adottare le misure necessarie affinché gli atti intenzionali di cui alle lettere che lo compongono siano punibili come reato. L'articolo elenca il furto o altra illecita appropriazione di uno strumento di pagamento materiale diverso dai contanti (lettera a)); la contraffazione o falsificazione fraudolenta di uno strumento di pagamento materiale diverso dai contanti (lettera b)); il possesso di uno strumento di pagamento materiale diverso dai contanti rubato o altrimenti ottenuto mediante illecita appropriazione, o contraffatto o falsificato a fini di utilizzazione fraudolenta (lettera c)); l'atto di procurare per sé o per altri, compresi la ricezione, l'appropriazione, l'acquisto, il trasferimento, l'importazione, l'esportazione, la vendita, il trasporto e la distribuzione, di uno strumento di pagamento materiale diverso dai contanti rubato, contraffatto o falsificato, a fini di utilizzazione fraudolenta (lettera d)).

Anche se l'articolo 4 sembra essere stato recepito quasi sempre in modo pressoché letterale, in alcuni casi il testo nazionale solleva perplessità per quanto concerne gli specifici atti di procurare per sé o per altri uno strumento di pagamento materiale diverso dai contanti rubato, contraffatto o falsificato a fini di utilizzazione fraudolenta.

c) Reati connessi all'utilizzazione fraudolenta di strumenti di pagamento immateriali diversi dai contanti

L'articolo 5 della direttiva configura come reato le condotte connesse all'utilizzazione fraudolenta di strumenti di pagamento immateriali diversi dai contanti. Dall'analisi sembra che tale articolo non abbia creato problemi di recepimento. Nella maggior parte dei casi la disposizione nazionale si applica sia agli strumenti di pagamento materiali diversi dai contanti, sia a quelli immateriali. Circa la metà degli Stati membri ha recepito l'articolo 5 della direttiva mediante disposizioni più generali (BE, BG, DE, EE, FI, HR, FR, LV, PL, SE, SK) e più della metà di essi lo ha recepito mediante una disposizione riguardante

specificamente l'utilizzazione fraudolenta di strumenti di pagamento diversi dai contanti (AT, CY, CZ, EL, ES, HU, IT, LT, LU, NL, PT, RO, SI).

d) Frode connessa ai sistemi di informazione

L'articolo 6 della direttiva obbliga gli Stati membri a provvedere affinché 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, sia punibile come reato se commesso intenzionalmente ostacolando, senza diritto, il funzionamento di un sistema di informazione o interferendo con esso (articolo 6, lettera a)); oppure introducendo, alterando, cancellando, trasmettendo o sopprimendo, senza diritto, dati informatici (articolo 6, lettera b)). Tutti gli Stati membri hanno recepito l'articolo 6.

e) Mezzi utilizzati per commettere i reati

L'articolo 7 della direttiva impone agli Stati membri di adottare le misure necessarie affinché siano punibili come reati la fabbricazione, l'ottenimento per sé o per altri, o la messa a disposizione di un dispositivo o di uno strumento, di dati informatici o di altri mezzi principalmente progettati o specificamente adattati al fine di commettere uno dei reati di cui all'articolo 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.

La grande maggioranza degli Stati membri ha recepito l'articolo 7 della direttiva (AT, CY, CZ, DE, EE, ES, FI, FR, HR, IT, LT, LV, NL, RO, SE, SI, SK).

Sei paesi hanno recepito l'articolo 7 della direttiva mediante disposizioni che rinviano a disposizioni più ampie, riguardanti reati generali come il furto oppure gli strumenti finanziari e i mezzi di pagamento (BG, FI, FR, LV, SE, SK). 17 paesi hanno recepito tale articolo mediante una disposizione specifica sugli strumenti utilizzati per commettere i diversi reati contemplati dalla direttiva relativi agli strumenti di pagamento materiali o immateriali diversi dai contanti (AT, CY, CZ, DE, EE, EL, ES, HR, HU, IT, LT, LU, MT, NL, PL, RO, SI).

Cinque Stati membri sembrano aver incontrato difficoltà nel recepimento (BE, BG, HU, PL, PT).

2.3 Norme generali relative ai reati

a) Istigazione, favoreggiamento, concorso e tentativo

A norma dell'articolo 8, paragrafo 1, della direttiva, gli Stati membri devono provvedere affinché l'istigazione, il favoreggiamento e il concorso in relazione ai reati di cui agli articoli da 3 a 7 siano punibili come reati.

Tutti gli Stati membri hanno recepito questa disposizione. La grande maggioranza degli Stati membri ha recepito la direttiva mediante un articolo preesistente concernente l'istigazione, il favoreggiamento e il concorso in generale (AT, BE, BG, CZ, DE, EE, EL, ES, FI, FR, HR, HU, IT, LT, LU, LV, NL, PL, PT, RO, SE, SI, SK). Due Stati membri hanno invece deciso di emanare una nuova disposizione che si applica unicamente nel contesto dei reati previsti dalla direttiva (CY, MT).

L'articolo 8, paragrafo 2, prima frase, della direttiva impone agli Stati membri di provvedere affinché il tentativo di commettere un reato di cui all'articolo 3, all'articolo 4, lettere a), b) e d), all'articolo 5, lettere a) e b), e all'articolo 6 sia punibile come reato. Risulta che tutti gli

Stati membri, ad eccezione di BE, LU e SI, abbiano recepito tale disposizione in modo completo.

Anche in questo caso la maggior parte degli Stati membri ha recepito la direttiva mediante una disposizione precedentemente esistente applicabile al tentativo in generale (AT, BG, CZ, EE, EL, ES, FR, HR, HU, IT, LT, LV, NL, PL, PT, SE, SK). Gli altri hanno inserito il tentativo in una misura speciale di recepimento (CY, DE, FI, MT, RO).

Gli Stati membri devono altresì garantire almeno che il tentativo di procurare in modo fraudolento, per sé o per altri, uno strumento di pagamento immateriale diverso dai contanti ottenuto illecitamente, contraffatto o falsificato (con riferimento all'articolo 5, lettera d)) sia punibile come reato (articolo 8, paragrafo 2, seconda frase).

Dalla valutazione è emerso che in due Stati membri (HR, SI) la criminalizzazione del tentativo può essere soggetta a limitazioni non previste dalla direttiva.

Tutti gli altri Stati membri hanno recepito le pertinenti disposizioni della direttiva, mediante un articolo sul tentativo in generale (AT, BE, BG, CZ, IT, EE, EL, ES, FR, HU, LT, LU, LV, NL, PL, PT, SE, SK) oppure mediante una misura speciale di recepimento (CY, DE, FI, MT, RO).

b) Sanzioni

L'articolo 9 stabilisce che i reati di cui agli articoli da 3 a 8 sono punibili con sanzioni penali effettive, proporzionate e dissuasive e indica la pena detentiva massima per i diversi reati.

Sebbene gli Stati membri abbiano generalmente recepito l'articolo 9 della direttiva, dalla valutazione sono emerse possibili problematiche relative all'ambito di applicazione della definizione per quanto riguarda l'articolo 9, paragrafo 2, in HR e l'articolo 9, paragrafo 6, in BE, CZ, HR e HU.

Il confronto tra le sanzioni stabilite dagli Stati membri per i diversi reati è complesso, in quanto i reati sono disciplinati sia da disposizioni generali che da disposizioni specifiche. Gli Stati membri che hanno recepito la direttiva mediante disposizioni su reati generali si sono basati su varie disposizioni nazionali per configurare come reati i singoli atti vietati dalla direttiva. Di conseguenza vi è una pluralità di sanzioni massime applicabili a uno specifico reato e la loro effettiva entità dipende dal singolo caso, dall'approccio seguito dagli organi giurisdizionali e dalle norme nazionali sul cumulo delle sanzioni. A titolo di esempio, in PL la norma prevede che un unico atto possa configurare un unico reato. Nel caso in cui una condotta presenti caratteristiche riconducibili a due o più disposizioni del diritto penale, l'organo giurisdizionale deve considerare un solo reato specifico. Al contrario in BG, nei casi in cui la parte speciale del codice penale prevede l'irrogazione di due o più sanzioni cumulativamente per un determinato reato, l'organo giurisdizionale determina l'entità di ciascuna sanzione in modo tale che l'insieme delle stesse sia conforme agli obiettivi generali della pena.

Inoltre le disposizioni possono contemplare circostanze aggravanti a cui possono essere associati limiti di pena più elevati e quindi sanzioni più severe. La sanzione massima dipende pertanto dalle modalità di commissione del reato. Ad esempio, in HR la disposizione generale sull'appropriazione indebita prevede una sanzione massima di cinque anni di reclusione. Tuttavia, se l'autore del reato ha fatto ricorso alla forza, la sanzione massima è di 10 anni di reclusione, mentre se la condotta ha provocato un notevole guadagno materiale l'autore del reato è punibile con una pena detentiva fino a 12 anni. In DE la falsificazione degli strumenti

di pagamento materiali diversi dai contanti è soggetta a pene detentive della durata massima di cinque anni. Tuttavia, se l'autore del reato ha agito con finalità commerciali, la sanzione massima è di 10 anni di reclusione.

Dalla valutazione è anche emerso che nella maggior parte dei casi le soglie previste dalla normativa nazionale sono più rigorose di quelle fissate dalla direttiva. La differenza può essere considerevole: la falsificazione di denaro è punibile con la reclusione fino a 15 anni in BG e in LU e fino a 25 anni in PL. Soltanto due Stati membri prevedono sanzioni massime identiche (o molto simili) a quelle previste dalla direttiva (AT, MT).

c) Responsabilità delle persone giuridiche

Dalla valutazione è emerso che 16 Stati membri hanno recepito l'articolo 10 della direttiva mediante una disposizione generale già esistente dei rispettivi codici penali (AT, CZ, BE, BG, DE, EE, ES, FR, HR, HU, LU, LV, NL, PT, RO, SE), mentre nove Stati membri lo hanno recepito attraverso una legge specifica sulla responsabilità delle persone giuridiche nel contesto della direttiva (CY, EL, FI, IT, LT, MT, PL, SI, SK).

d) Sanzioni per le persone giuridiche

L'articolo 11 della direttiva impone agli Stati membri di stabilire sanzioni effettive, proporzionate e dissuasive sotto forma di sanzioni pecuniarie penali o non penali anche per le persone giuridiche. Tutti gli Stati membri hanno istituito tali sanzioni.

L'articolo 11 dà agli Stati membri la facoltà di prevedere varie sanzioni specifiche per le persone giuridiche, quali l'esclusione dal godimento di un beneficio pubblico o provvedimenti giudiziari di scioglimento. Sei Stati membri non si sono avvalsi della facoltà di cui all'articolo 11 della direttiva (AT, BG, EE, FI, NL, SE). Gli altri 19 paesi hanno recepito l'intero articolo 11 o parti di esso (BE, CY, CZ, DE, EL, ES, FR, HR, HU, IT, LT, LU, LV, MT, PL, PT, RO, SI, SK).

e) Giurisdizione

L'articolo in questione, che obbliga gli Stati membri a stabilire la giurisdizione per i reati commessi sul proprio territorio o dai propri cittadini, è stato recepito nelle disposizioni generali del codice penale nazionale o del codice di procedura penale nazionale in tutti gli Stati membri. Pertanto il principio di territorialità e il principio della cittadinanza attiva sono di applicazione generale e non riguardano in modo specifico i reati disciplinati dalla direttiva. L'articolo 12 è stato recepito anche da CY nella legge nazionale sulla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti e da PT nella legge sulla criminalità informatica.

Tutti gli Stati membri hanno recepito l'articolo 12, paragrafo 1, lettere a) e b).

L'articolo 12, paragrafo 3, consente a uno Stato membro di stabilire la giurisdizione per un reato di cui agli articoli da 3 a 8 della direttiva commesso al di fuori del suo territorio, qualora, tra l'altro, a) il reato sia commesso da una persona che risiede abitualmente nel suo territorio; b) il reato sia commesso a vantaggio di una persona giuridica stabilita nel suo territorio; o c) il reato sia stato commesso contro uno dei suoi cittadini o contro una persona che risiede abitualmente nel suo territorio. Quattordici Stati membri (BE, CY, CZ, DE, EL, ES, FI, HR, LT, LV, MT, NL, SE, SK) si sono avvalsi della facoltà di cui all'articolo 12, paragrafo 3, lettera a); 12 Stati membri (BE, CY, CZ, EL, FI, LV, MT, NL, PL, PT, SI, SK) hanno recepito l'articolo 12, paragrafo 3, lettera b); e 16 Stati membri (AT, BG, CY, CZ, DE,

EE, EL, FI, FR, HR, HU, LV, MT, RO, SE, SI) hanno esteso la propria giurisdizione a norma dell'articolo 12, paragrafo 3, lettera c). Per quanto riguarda tale lettera c), BG, DE, EE, HU, RO e SI hanno stabilito la propria giurisdizione nei confronti di un reato commesso al di fuori del proprio territorio qualora il reato sia stato commesso (unicamente) contro uno dei loro cittadini, escludendo quindi le persone che risiedono abitualmente nei loro territori. AT prevede l'esercizio dell'azione penale da parte del sistema di giustizia penale nazionale per i reati commessi all'estero se l'autore e la vittima sono austriaci. CY, CZ, EL, FI, LV e MT si sono avvalse di tutte e tre le disposizioni facoltative di cui all'articolo 12, paragrafo 3.

2.4 Aspetti operativi

a) Efficacia delle indagini e cooperazione

In tutti gli Stati membri gli strumenti per indagare e perseguire i reati di cui agli articoli da 3 a 8 non figurano esplicitamente nella normativa di recepimento della direttiva, ma piuttosto nella legislazione generica, ad esempio nei codici di procedura penale. In genere la possibilità di utilizzare uno strumento di indagine in un determinato caso è legata alla sanzione prevista per il reato in questione; pertanto, come già indicato nella disposizione della direttiva, gli strumenti di indagine utilizzati per contrastare la criminalità organizzata o altre forme gravi di criminalità saranno disponibili anche per indagare e perseguire i reati di cui alla direttiva stessa. Nella maggior parte dei casi le disposizioni di legge pertinenti e/o la Costituzione sanciscono l'eccezionalità di alcuni strumenti di indagine e il requisito della proporzionalità rispetto al reato.

Conformemente all'articolo 13, paragrafo 2, della direttiva, le informazioni relative ai reati di cui agli articoli da 3 a 8 dovrebbero pervenire senza indugio alle autorità che indagano o perseguono tali reati. In altri termini, le autorità di contrasto e le altre autorità competenti dovrebbero poter accedere tempestivamente alle informazioni utili per svolgere le indagini e perseguire i reati di cui alla direttiva (considerando 22). I codici di procedura penale prevedono spesso vari sistemi di comunicazione atti a consentire la comunicazione efficiente e rapida dei reati (ai sensi degli articoli da 3 a 8 della direttiva). Tali sistemi di comunicazione prevedono, ad esempio: il dovere di comunicazione in capo agli organismi e alle autorità pubblici; un sistema di denuncia delle irregolarità; una procedura di reclamo; l'obbligo dei fornitori di servizi di pagamento di comunicare gravi incidenti operativi o di sicurezza; e il diritto dei privati di comunicare gli incidenti. Leggi più specifiche possono inoltre garantire la massima tempestività della comunicazione degli incidenti di sicurezza (comprese le segnalazioni di reati gravi, come l'acquisizione non autorizzata, la falsificazione e l'alterazione di un mezzo di pagamento) alle autorità competenti. AT, CZ, LT, FI, MT e PT hanno comunicato l'esistenza di leggi di questo tipo.

Nella maggior parte dei casi la condizione secondo cui le informazioni trasmesse devono pervenire "senza indugio" alle autorità competenti non è stata recepita esplicitamente.

b) Scambio di informazioni

Lo scambio di informazioni tra le autorità nazionali di contrasto al fine di indagare e perseguire i reati, compresi quelli di cui agli articoli da 3 a 8 della direttiva, può essere agevolato tramite punti di contatto operativi (considerando 26). L'articolo 14, paragrafo 1, prima frase, della direttiva prevede infatti che gli Stati membri istituiscano tali punti di contatto e che questi ultimi siano disponibili ventiquattr'ore su ventiquattro, sette giorni su

sette. Inoltre la seconda frase obbliga gli Stati membri a predisporre procedure per trattare tempestivamente le richieste urgenti di assistenza e rispondervi entro otto ore, indicando almeno se alla richiesta sarà data una risposta, la forma di tale risposta e il termine stimato entro il quale sarà fornita.

Gli Stati membri seguenti hanno deciso di avvalersi di un punto di contatto operativo esistente per gli scopi descritti nella direttiva: AT, BE, CY, EE, EL, ES, FR, HU, IT, LT, LV, NL, PL, PT, SE.

La tabella 1 fornisce una panoramica dei punti di contatto istituiti. Non sono stati individuati punti di contatto in BG, CZ, LU, SI, HR.

Tabella 1 Punti di contatto operativi

SM	Punto di contatto		SM	Punto di contatto
AT	Ufficio federale della polizia criminale		**EE**	Ministero della Giustizia
BE	Direzione per le informazioni operative di polizia		**FI**	Ufficio nazionale di intelligence
BG	N/A		**FR**	Divisione relazioni internazionali della direzione centrale della polizia giudiziaria
CY	Polizia di Cipro		**HR**	N/A
CZ	N/A		**HU**	Centro internazionale per la cooperazione tra le forze di polizia) (NEBEK)
DE	16 uffici della polizia criminale dello Stato e un ufficio federale della polizia criminale — Punti di contatto centrali per la criminalità informatica		**MT**	Polizia di Malta
EL	Polizia ellenica (divisione per la cooperazione internazionale di polizia)		**ES**	Cellula di coordinamento di emergenza
IT	Sala operativa internazionale del Servizio per la cooperazione internazionale di polizia		**NL**	Centro nazionale per l'assistenza giudiziaria internazionale (LIRC)
LT	Seconda divisione del consiglio per la gestione delle forze del dipartimento di polizia presso il ministero dell'Interno della Repubblica di Lituania e Consiglio per le relazioni internazionali dell'ufficio lituano di polizia criminale		**PL**	Direzione generale della polizia
LV	Polizia nazionale		**PT**	Polizia criminale
RO	Sezione dell'ufficio del procuratore generale incaricata dell'azione penale e delle indagini penali		**SE**	Autorità di polizia
SI	N/A		**SK**	Ufficio di polizia giudiziaria del corpo di polizia della Repubblica slovacca

L'articolo 14, paragrafo 1, seconda frase, della direttiva è stato attuato concretamente in alcuni Stati membri. Non è stato possibile reperire informazioni sulle procedure applicabili alle richieste urgenti in BE, BG, CZ, LV, RO, FR, HR, LU, NL, PL, SE, SK.

c) Comunicazione dei reati

Gli Stati membri sono anche tenuti a mettere a disposizione adeguati canali di comunicazione. Tali canali, destinati alla comunicazione di sospetti di frode o, più in generale, alla denuncia di eventuali reati, possono essere stabiliti da atti legislativi. In molti casi gli Stati membri hanno istituito l'obbligo di comunicazione di un reato per determinate categorie di persone (fisiche e giuridiche) (strettamente in linea con l'articolo 15, paragrafo 2), mentre per le

vittime e le "persone estranee ai fatti" hanno previsto la facoltà (ma non l'obbligo) di comunicazione. Queste disposizioni giuridiche sono generalmente integrate da norme di attuazione pratica.

In tutti gli Stati membri esiste la possibilità di presentare comunicazioni scritte o orali alla polizia e/o alla magistratura. Inoltre alcuni Stati membri hanno predisposto canali di comunicazione supplementari:

In AT la legge federale prevede vari sistemi di comunicazione atti a consentire la comunicazione efficiente e rapida dei reati di cui agli articoli da 3 a 8 della direttiva, tra cui: 1) il dovere di comunicazione in capo agli organismi e alle autorità pubblici; 2) il sistema di denuncia delle irregolarità adottato dall'ufficio della procura preposto alla lotta contro i reati economici e la corruzione; 3) il sistema di denuncia delle irregolarità adottato dall'autorità per i mercati finanziari; e 4) l'obbligo per i fornitori di servizi di pagamento di comunicare gli incidenti operativi o di sicurezza gravi. Presso l'ufficio della polizia criminale federale è stato istituito un ufficio specializzato per la comunicazione dei reati informatici. Inoltre il ministero federale dell'Interno collabora con la camera federale dell'economia, per cui sono in corso varie iniziative tramite messaggi di posta elettronica e campagne al fine di motivare e incoraggiare il pubblico a comunicare i casi di violazione della legge.

In BE il ministero dell'Economia gestisce un punto di contatto unico per le vittime di frodi, truffe, inganni e raggiri. Inoltre è stato istituito per legge e messo a disposizione dall'Autorità per i servizi e i mercati finanziari un canale di denuncia delle irregolarità per tutte le denunce relative a prodotti e servizi di credito o di investimento.

A CY la polizia cipriota, insieme alla Banca centrale di Cipro e all'autorità nazionale per la sicurezza delle reti e dei sistemi di informazione, sono state formalmente designate mediante una misura legislativa quali autorità nazionali competenti incaricate dell'istituzione di adeguati canali di segnalazione e di comunicazione.

In CZ il diritto penale prevede l'obbligo di comunicazione da parte delle autorità statali.

In DE i soggetti obbligati sono tenuti a comunicare senza indebito ritardo le operazioni sospette. Inoltre a livello federale sono state adottate misure non legislative, tra cui un partenariato istituzionalizzato pubblico-privato al fine di individuare, prevenire, indagare o perseguire i reati di cui agli articoli da 3 a 8 della direttiva, nonché una piattaforma per lo scambio di informazioni.

In EL, oltre ai canali generali di comunicazione, il governo greco ha istituito un servizio statale online tramite il quale i cittadini possono presentare direttamente denunce relative a reati commessi online. Inoltre gli enti creditizi e gli altri fornitori di servizi di pagamento devono comunicare alla Banca centrale greca (che è competente per tali denunce) qualsiasi incidente di frode immediatamente dopo averlo riscontrato.

In Spagna, accanto ai canali generali di comunicazione dei reati, esiste un canale di comunicazione curato dalla Banca di Spagna in collaborazione con l'Istituto nazionale per la cibersicurezza.

La normativa italiana garantisce la tempestività nella comunicazione al pubblico ministero, da parte della polizia giudiziaria, della notizia di reato acquisita di propria iniziativa o a seguito di denuncia o querela. È altresì incoraggiata la condivisione delle informazioni attraverso le piattaforme digitali.

La LT dispone di molteplici canali di comunicazione dei reati di cui agli articoli da 3 a 8 della direttiva, vale a dire una pagina web (il portale e-Police), il numero telefonico di emergenza generale 112, la comunicazione di persona, per posta elettronica, mediante SMS, tramite l'applicazione mobile e-Police o con altri mezzi automatici. I fornitori di servizi di pagamento, le istituzioni finanziarie e gli altri soggetti obbligati, la Banca di Lituania e il servizio per le indagini sui reati finanziari sono tenuti a notificare alle autorità di contrasto competenti i ragionevoli sospetti di atti criminali e/o di altri atti illeciti.

In LU è disponibile un sito web che illustra le modalità di comunicazione delle frodi. La commissione di controllo del settore finanziario ha stabilito orientamenti per individuare le frodi finanziarie, ma chiede anche a tutti gli istituti sottoposti alla sua vigilanza di comunicare quanto prima eventuali frodi e incidenti dovuti ad attacchi informatici esterni.

In RO è previsto l'obbligo di comunicazione per i funzionari pubblici e per le persone che ricoprono cariche dirigenziali presso le autorità pubbliche, per le persone che prestano servizi di interesse pubblico e per le persone che operano nell'ambito di organismi di controllo e di vigilanza.

In SI il dovere di comunicare un reato incombe a tutte le autorità statali e a tutte le organizzazioni investite di pubblici poteri.

In FR la piattaforma *Perceval*, istituita con atto giuridico, consente alle vittime di comunicare frodi e contraffazioni di carte bancarie. Esiste una piattaforma analoga per le comunicazioni relative alla criminalità informatica. Inoltre l'applicazione di sanzioni nei confronti di qualsiasi persona (fisica o giuridica) che non impedisca, con il proprio intervento immediato, la commissione di un reato determina un obbligo generale di comunicazione.

In HU l'obbligo di comunicare un reato è previsto solo per i membri delle autorità, i funzionari pubblici e gli organismi professionali istituiti per legge. La Banca nazionale ungherese incoraggia sul suo sito web le istituzioni finanziarie a comunicare, sotto forma di parere, eventuali sospetti di frode.

A MT il punto di contatto nazionale incoraggia la comunicazione, in particolare da parte da parte delle istituzioni finanziarie, dei sospetti di frode e di falsificazioni di mezzi di pagamento diversi dai contanti.

Oltre al canale di comunicazione per la denuncia delle irregolarità istituito per legge, in PT è disponibile un sistema di comunicazione dei reati informatici "con un solo clic", in cui è possibile selezionare un link che apre istantaneamente un messaggio di posta elettronica indirizzato alle autorità competenti.

In SE alcuni tipi di reati, quali le frodi commesse con carte di credito, possono essere comunicati anche tramite il servizio elettronico dell'autorità di polizia. Inoltre gli operatori delle attività bancarie e finanziarie sono obbligati a comunicare all'autorità di polizia le attività sospette connesse a potenziali casi di riciclaggio di capitali o di finanziamento del terrorismo, o a beni comunque derivanti dal compimento di atti criminali. A ciò si aggiunge il dialogo costante tra i soggetti attivi nelle operazioni bancarie e finanziarie e il centro nazionale antifrode dell'autorità di polizia.

Le disposizioni giuridiche in SK stabiliscono l'obbligo delle autorità pubbliche e di altre persone giuridiche di comunicare immediatamente i reati alle autorità di contrasto (e indicano le relative procedure). Vi sono anche obblighi di comunicazione relativi al riciclaggio di capitali in capo ai soggetti obbligati e in particolare alle banche.

In NL e in PL sono state invece intraprese azioni non legislative per l'attuazione dell'articolo 15 della direttiva. Le linee dei servizi di polizia dei Paesi Bassi e il sito web della polizia forniscono un canale adeguato per comunicare alle autorità le frodi che riguardano mezzi di pagamento diversi dai contanti. Il governo dei Paesi Bassi si è impegnato a incoraggiare le istituzioni finanziarie e altre persone giuridiche a comunicare qualsiasi sospetto di frode. Tale impegno è testimoniato, ad esempio, dall'esistenza di un front office per le frodi finanziarie operativo in tutte le unità di polizia dei Paesi Bassi. Inoltre quattro importanti banche e i gestori di carte ICS hanno firmato un patto con la polizia per la lotta congiunta contro le frodi (bancarie) e il phishing. In PL le comunicazioni di reati sono prese in carico 24 ore su 24, 7 giorni su 7, da tutte le unità di polizia. Inoltre, data la natura dei reati commessi mediante l'utilizzazione delle tecnologie informatiche, è prevista la possibilità di rivolgersi direttamente a un'unità organizzativa specializzata della direzione centrale della polizia. Al fine di accelerare il più possibile la collaborazione con il settore bancario, è stato inoltre istituito un canale di cooperazione tra l'ufficio per la lotta alla criminalità informatica della direzione centrale della polizia e il centro di sicurezza bancaria dell'associazione bancaria polacca.

L'articolo 15, paragrafo 2, della direttiva non è stato recepito in BG, EE, HR.

2.5 Sostegno alle vittime e prevenzione

a) Assistenza e sostegno alle vittime

L'assistenza e il sostegno alle persone fisiche e alle persone giuridiche i cui dati personali sono stati utilizzati in maniera fraudolenta sono garantiti dall'articolo 16, paragrafo 1, della direttiva. Tra le misure previste dovrebbero figurare: a) l'offerta di informazioni e consigli specifici sulla protezione dalle conseguenze negative di tale reato e b) la messa a disposizione di un elenco delle istituzioni che si occupano specificamente di diversi aspetti del reato connesso all'identità e del sostegno alle vittime.

Nella stessa ottica, le persone giuridiche vittime dei reati di cui agli articoli da 3 a 8 di tale direttiva dovrebbero avere accesso alle informazioni riguardanti a) le procedure per la presentazione di una denuncia, b) il diritto di ricevere informazioni sul caso, c) le procedure disponibili per presentare una denuncia se l'autorità competente non rispetta i diritti della vittima nell'ambito del procedimento penale e d) i referenti a cui rivolgersi per comunicazioni sul proprio caso (articolo 16, paragrafo 3, della direttiva).

I codici di procedura penale della maggior parte degli Stati membri contengono norme concernenti le vittime e i relativi diritti, comprese alcune disposizioni specifiche sui diritti delle vittime all'informazione e all'assistenza durante il procedimento, sul diritto alla consulenza giuridica e sul diritto di presentare denuncia. Spesso una legge specifica di recepimento della direttiva integra quanto già stabilito nel codice di procedura penale. Le persone giuridiche sono generalmente oggetto di disposizioni di legge distinte nell'ambito del codice di procedura penale o di altri testi. Inoltre è disponibile una serie di campagne d'informazione, opuscoli, siti web dedicati, circolari ecc. per assistere e sostenere le vittime dei reati di cui agli articoli da 3 a 8 della direttiva. È il caso di AT, BE (per quanto riguarda l'articolo 16, paragrafo 1), CY, CZ, DE, IT, LT, LU (per quanto riguarda l'articolo 16, paragrafo 1), LV (per quanto riguarda l'articolo 16, paragrafo 3), RO, SI (per quanto riguarda l'articolo 16, paragrafo 3), EE, FI (per quanto riguarda l'articolo 16, paragrafo 1), FR (per quanto riguarda l'articolo 16, paragrafo 1), HR, HU, NL, PL (per quanto riguarda l'articolo 16, paragrafo 3), PT, SE e SK. Ad eccezione di MT, in nessun caso si è proceduto al recepimento

letterale o quasi letterale dell'articolo 16, paragrafo 1, e/o dell'articolo 16, paragrafo 3, della direttiva.

L'elenco delle strutture di consulenza accreditate che forniscono assistenza alle vittime al quale si fa riferimento all'articolo 16, paragrafo 1, lettera b), della direttiva è di norma disponibile online ed è pertanto attuato nella pratica.

b) Prevenzione

L'articolo 17 sulla prevenzione impone agli Stati membri di adottare azioni adeguate, ad esempio campagne di informazione e di sensibilizzazione e programmi di ricerca e d'istruzione. Tale sezione si basa su una valutazione delle informazioni notificate dagli Stati membri alla Commissione e su una ricerca open source su Internet volta a esaminare l'esistenza di misure di prevenzione. Come descritto nella tabella 2, le azioni di prevenzione, laddove riscontrate, riguardano principalmente la criminalità informatica e le frodi online. Tuttavia in alcuni paesi sono disponibili anche informazioni sulla prevenzione delle frodi, solitamente fornite dalla polizia.

Tabella 2 Azioni di prevenzione

SM	Azioni
AT	La polizia federale fornisce periodicamente informazioni sul proprio sito web e sui social network su come proteggersi dalle frodi. La cooperazione con i portatori di interessi, tra cui la camera di commercio, è sostenuta e attuata nel quadro di progetti di commercio elettronico.
BE	Diversi siti web, come quelli gestiti dal *Centre for Cybersecurity Belgium* (CCB), contengono materiale di consulenza/sensibilizzazione. Tramite una ricerca su Internet è stato possibile individuare alcuni esempi di cooperazione con i portatori di interessi; ad esempio l'organizzazione che rappresenta il settore finanziario ha collaborato con la procura di Bruxelles (*parquet*) per elaborare materiale di sensibilizzazione.
BG	Nel 2021 è stata avviata una campagna di contrasto al fenomeno dei "prestaconto" in Bulgaria, curata dall'associazione delle banche e condotta congiuntamente con la direzione generale "Lotta alla criminalità organizzata" e la procura. La direzione generale ha anche lanciato una campagna sul phishing.
CY	La sottodivisione di polizia responsabile della lotta alla criminalità informatica fornisce sul suo sito web informazioni e consulenza su questioni quali le frodi digitali, nonché informazioni su eventi futuri, ad esempio campagne di sensibilizzazione. Un esempio è la campagna di informazione sulla sicurezza delle informazioni condotta dalla polizia, dalle banche centrali, dall'associazione delle banche e dall'autorità di sicurezza digitale.
DE	L'ufficio federale della polizia criminale (BKA) fornisce sul proprio sito web una panoramica delle misure destinate ai partenariati istituzionalizzati pubblico-privato volti a individuare, prevenire, indagare o perseguire i reati contemplati dalla direttiva; tra questi figura il partenariato tra l'ufficio federale della polizia criminale (BKA), l'ufficio federale per la sicurezza delle informazioni (BSI) e il *German Competence Centre against Cyber Crime e.V.* (G4C), un'associazione di istituzioni finanziarie e società del settore della sicurezza informatica. Il BKA ha inoltre lanciato *Cybercrime Conference C³*, una piattaforma di scambio per autorità, imprese, mondo scientifico e politico. Il G4C realizza anche opuscoli informativi e attività di formazione. Infine il BKA partecipa a misure di prevenzione nel settore della criminalità informatica a livello dei Länder, mentre a livello nazionale è in collegamento con altre autorità e organizzazioni di polizia e non di polizia (portatori di interessi) e sta intensificando la cooperazione soprattutto sui temi di maggiore attualità.
FR	Il ministero dell'Interno pubblica informazioni sulla prevenzione in campo informatico. Le piattaforme disponibili per la comunicazione dei reati informatici comprendono anche messaggi di prevenzione e il servizio nazionale di informazione e comunicazione della polizia (SICoP). Tra gli altri esempi figurano gli orientamenti emanati dalla Banca di Francia o la guida sulla prevenzione delle frodi pubblicata dalla task force nazionale per la lotta contro le frodi, che raggruppa diverse autorità amministrative e di contrasto.

EL	Attraverso campagne televisive, conferenze divulgative e informazioni online, la divisione di polizia responsabile della lotta alla criminalità informatica e la direzione centrale della polizia si adoperano attivamente per informare il pubblico, sensibilizzarlo e ridurre il rischio che le persone subiscano frodi.
ES	L'istituto nazionale spagnolo per la cibersicurezza e l'Agenzia delle entrate spagnola forniscono sui rispettivi siti web informazioni pertinenti a prevenire il phishing, il ransomware ecc. nei contesti aziendali.
HR	Il ministero dell'Interno fornisce informazioni online sulle frodi su Internet e gestisce un canale Youtube dedicato a "frodi e sicurezza informatica", contenente video sulle truffe informatiche.
IT	Il Dipartimento del Tesoro, che ha il compito di prevenire le frodi sui mezzi di pagamento, sta già promuovendo una serie di iniziative a livello locale in collaborazione con le amministrazioni locali e il sistema universitario, organizzando seminari e workshop rivolti alle categorie interessate dalla falsificazione monetaria, compresi i cittadini.
LT	Informazioni sulla prevenzione sono disponibili sul sito web dell'autorità di regolamentazione delle comunicazioni in relazione alle frodi online e sul sito web della polizia per quanto riguarda le tipologie più comuni di frodi informatiche. Inoltre uno degli obiettivi della strategia nazionale in materia di criminalità informatica è rafforzare la prevenzione e il controllo di tale fenomeno, in particolare sviluppando una cooperazione efficace tra le autorità di contrasto e altri portatori di interessi.
LV	La commissione per i mercati finanziari e dei capitali ha sviluppato vari strumenti Internet per fornire informazioni e orientamenti in materia di sicurezza finanziaria e frodi. Inoltre sono state organizzate varie campagne in collaborazione con la polizia di Stato e il centro per la tutela dei diritti dei consumatori.
NL	Sono in atto misure quali il *Fraudehelpdesk* (servizio di assistenza telefonica contro le frodi), un'organizzazione sovvenzionata dal governo olandese alla quale è possibile comunicare i casi di azioni fraudolente. Il *Fraudehelpdesk* fa parte della SAFECIN (Fondazione per la lotta alla criminalità finanziaria ed economica nei Paesi Bassi), una fondazione a partecipazione governativa.
SE	È mantenuto un dialogo costante tra i soggetti attivi nelle operazioni bancarie e finanziarie e il centro nazionale antifrode dell'autorità di polizia (NBC). Inoltre l'NBC collabora, anche a fini di prevenzione della criminalità, con soggetti quali gli attori del commercio elettronico. Nell'ambito di tali contatti è sottolineata l'importanza di comunicare le frodi alla polizia.

Per dieci Stati membri (CZ, EE, FI, HU, MT, PL, PT, RO, SI, SK) non sono state reperite informazioni su azioni di prevenzione adeguate e sulla loro attuazione pratica, anche se in MT e RO l'obbligo in questione trova riscontro nei testi legislativi in una formulazione molto vicina a quella della direttiva.

3. Conclusione e sviluppi futuri

La direttiva ha determinato progressi sostanziali in termini di penalizzazione delle frodi e delle falsificazioni di mezzi di pagamento diversi dai contanti a un livello analogo in tutti gli Stati membri, il che facilita la cooperazione transfrontaliera fra le autorità di contrasto che indagano su questo tipo di reati. Gli Stati membri hanno modificato i codici penali e altre normative pertinenti, semplificato le procedure e avviato o migliorato programmi di cooperazione. La Commissione riconosce l'intenso impegno profuso dagli Stati membri per dare attuazione alla direttiva.

Tuttavia esistono ancora margini d'azione perché la direttiva possa raggiungere le sue piene potenzialità, se gli Stati membri garantiranno l'attuazione completa di tutte le sue disposizioni. In base all'analisi condotta finora, alcuni dei principali miglioramenti che gli Stati membri devono realizzare riguardano l'articolo 2, lettera d), recante la definizione di valuta virtuale; l'articolo 7, relativo ai mezzi utilizzati per commettere i reati, e l'articolo 8, paragrafo 2, sul tentativo; l'articolo 9, paragrafo 6, sulle sanzioni applicabili alle persone fisiche qualora il reato sia commesso nell'ambito di un'organizzazione criminale; l'articolo 14 sullo scambio di informazioni; e l'articolo 16 sull'assistenza e sul sostegno alle vittime.

La Commissione continuerà a fornire sostegno agli Stati membri ai fini dell'attuazione della direttiva. In particolare, nel 2023 sarà pubblicato un apposito invito a presentare proposte.

La Commissione si impegna a garantire che il recepimento sia completato in tutta l'UE e che le disposizioni siano attuate correttamente, anche monitorando la conformità delle misure nazionali rispetto alle corrispondenti disposizioni della direttiva. Ove necessario, la Commissione si avvarrà dei poteri di esecuzione di cui dispone in forza dei trattati e li eserciterà mediante l'avvio di procedure di infrazione.