Consiliul
Uniunii Europene

Bruxelles, 11 iulie 2023
(OR. en)

11761/23

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

NOTĂ DE ÎNSOȚIRE

Sursă:	Secretara Generală a Comisiei Europene, sub semnătura dnei Martine DEPREZ, Directoare
Data primirii:	10 iulie 2023
Destinatar:	Dna Thérèse BLANCHET, Secretară Generală a Consiliului Uniunii Europene
Nr. doc. Csie:	COM(2023) 363 final
Subiect:	RAPORT AL COMISIEI CĂTRE PARLAMENTUL EUROPEAN ȘI CONSILIU de evaluare a gradului în care statele membre au luat măsurile necesare pentru a se conforma Directivei (UE) 2019/713 privind combaterea fraudelor și a contrafacerii în legătură cu mijloacele de plată fără numerar și de înlocuire a Deciziei-cadru 2001/413/JAI a Consiliului

În anexă, se pune la dispoziția delegațiilor documentul COM(2023) 363 final.

Anexă: COM(2023) 363 final

COMISIA
EUROPEANĂ

Bruxelles, 10.7.2023
COM(2023) 363 final

RAPORT AL COMISIEI CĂTRE PARLAMENTUL EUROPEAN ȘI CONSILIU

de evaluare a gradului în care statele membre au luat măsurile necesare pentru a se conforma Directivei (UE) 2019/713 privind combaterea fraudelor și a contrafacerii în legătură cu mijloacele de plată fără numerar și de înlocuire a Deciziei-cadru 2001/413/JAI a Consiliului

1. Introducere

Fraudele și contrafacerea în legătură cu mijloacele de plată fără numerar, cum ar fi cardurile de credit sau de plată, constituie surse de venit pentru criminalitatea organizată și factori favorizanți pentru alte activități infracționale, precum terorismul, traficul de droguri și traficul de persoane. Aceste infracțiuni provoacă pierderi semnificative: valoarea totală a tranzacțiilor frauduloase cu carduri emise în cadrul zonei unice de plăți în euro (SEPA) s-a ridicat la 1,87 miliarde EUR în 2019[1]. Marea majoritate a tranzacțiilor frauduloase sunt asociate fraudelor realizate fără prezența cardului (*card-not-present* – CNP): în 2019, 80 % din valoarea fraudelor asociate cardurilor reprezintă operațiuni CNP, și anume plăți prin internet, poștă sau telefon[2]. Fraudele CNP au generat pierderi în valoare de 1,50 miliarde EUR în 2019, în creștere cu 4,3 % față de anul precedent[3].

Există o dimensiune transfrontalieră clară: Mai mult de jumătate din valoarea totală a fraudelor în 2019 a fost legată de tranzacțiile transfrontaliere din cadrul SEPA. Din punct de vedere geografic, tranzacțiile interne au reprezentat 89 % din valoarea tuturor tranzacțiilor cu cardul în 2019, dar numai 35 % din totalul tranzacțiilor frauduloase. Tranzacțiile transfrontaliere din cadrul SEPA au reprezentat 9 % din totalul tranzacțiilor cu cardul din punctul de vedere al valorii, dar 51 % din totalul fraudelor raportate[4].

Pentru combaterea acestor infracțiuni în mod eficace, statele membre trebuie să definească în comun actele care ar trebui considerate fraudă și contrafacere a mijloacelor de plată fără numerar. De asemenea, acestea trebuie să își armonizeze nivelurile sancțiunilor și să dețină mijloacele operaționale pentru semnalarea infracțiunilor și pentru realizarea schimburilor de informații între autorități. În consecință, la 17 aprilie 2019, Parlamentul European și Consiliul au adoptat Directiva 2019/713 („directiva”) privind combaterea fraudelor și a contrafacerii în legătură cu mijloacele de plată fără numerar și de înlocuire a Deciziei-cadru 2001/413/JAI a Consiliului[5]. Prezentul raport răspunde cerinței prevăzute la articolul 21 din directivă.

1.1. Obiectivele și domeniul de aplicare al directivei

Directiva urmărește să armonizeze sistemele de drept penal ale statelor membre[6] în domeniul fraudei și al contrafacerii mijloacelor de plată fără numerar și să contribuie la îmbunătățirea cooperării dintre autoritățile competente. În acest scop, aceasta stabilește norme minime privind definiția infracțiunilor și a sancțiunilor penale. Domeniul de aplicare al directivei este amplu, acoperind orice „dispozitiv, un obiect sau o înregistrare protejat(ă), nematerial(ă) sau material(ă) sau o combinație a acestora, altul (alta) decât monedele legale și care, singur(ă)

---

[1] Banca Centrală Europeană, *Seventh report on card fraud* (Al șaptelea raport privind frauda cu carduri), disponibil la adresa: https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202110~cac4c418e8.en.html

[2] Ibid.

[3] Ibid.

[4] Ibid.

[5] https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:32019L0713.

[6] În continuare și cu excepția cazului în care se indică altfel în mod explicit, prin „state membre” sau „toate statele membre” se înțelege statele membre vizate de directivă, și anume toate statele membre ale UE, cu excepția Danemarcei și a Irlandei, care nu au luat parte la adoptarea directivei, în conformitate cu Protocolul privind poziția Danemarcei, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene (TFUE) și, respectiv, în conformitate cu Protocolul nr. 21 privind poziția Regatului Unit și a Irlandei.

sau împreună cu o procedură sau un set de proceduri, permite deținătorului sau utilizatorului să transfere bani sau valoare monetară, inclusiv prin mijloace digitale de schimb", articolul 2 litera (a)[7]. De exemplu, o aplicație de plată mobilă coroborată cu procedura de autorizare (de exemplu, PIN) ar fi acoperită de această definiție. Aceasta include, de asemenea, monedele virtuale [articolul 2 litera (d) și articolul 6].

Directiva definește infracțiuni specifice, și anume:

- utilizarea frauduloasă a instrumentelor de plată fără numerar (articolul 3);
- infracțiuni legate de utilizarea frauduloasă a instrumentelor de plată fără numerar materiale (articolul 4);
- infracțiuni legate de utilizarea frauduloasă a instrumentelor de plată fără numerar nemateriale (articolul 5);
- frauda legată de sistemele informatice (articolul 6);
- furnizarea ilegală de instrumente utilizate pentru săvârșirea infracțiunilor (articolul 7).

În plus, directiva **extinde răspunderea penală** la instigarea și complicitatea la săvârșirea de către persoane fizice și/sau juridice a infracțiunilor menționate mai sus, precum și la tentativa de a săvârși infracțiunile în cauză (articolul 8).

Nivelurile minime ale **sancțiunilor** maxime pentru infracțiunile menționate în directivă sunt prevăzute la articolul 9.

Articolele următoare stabilesc condițiile minime pentru **răspunderea persoanelor juridice** (articolul 10) și sancțiuni, care includ amenzi penale sau de altă natură, și prezintă, cu titlu de exemplu, o listă a altor sancțiuni împotriva acestora (articolul 11).

Obiectivul articolului 12 este de a garanta că infractorii, astfel cum se prevede în directivă, sunt urmăriți penal în legătură cu infracțiunile prevăzute la articolele 3-8 din directivă. **Competența** unui stat membru trebuie stabilită dacă a) infracțiunea este săvârșită, în totalitate sau parțial, pe teritoriul său și/sau b) infractorul este un cetățean al său. Cu alte cuvinte, articolul 12 alineatul (1) litera (a) din directivă stabilește principiul teritorialității, în timp ce litera (b) conduce la principiul cetățeniei active.

Articolul 13 alineatul (1) din directivă prevede că **instrumentele pentru investigarea** și urmărirea penală a infracțiunilor menționate la articolele 3-8 ar trebui să fie eficace, proporționale și accesibile persoanelor, unităților și serviciilor responsabile. Informațiile privind infracțiunile menționate la articolele 3-8 ar trebui să parvină fără întârzieri nejustificate autorităților care investighează sau urmăresc penal aceste infracțiuni, în conformitate cu articolul 13 alineatul (2) din directivă.

În ceea ce privește schimbul de informații, articolul 14 impune statelor membre să se asigure că dispun de **puncte operaționale naționale de contact** disponibile 24 de ore pe zi, șapte zile pe săptămână, astfel încât acestea să poată răspunde în termen de cel mult opt ore la orice cerere urgentă de asistență.

În plus, articolul 15 alineatul (1) din directivă impune statelor membre să instituie canale adecvate de **semnalare fără întârzieri nejustificate a autorităților publice cu privire la infracțiunile** menționate la articolele 3-8. În special, instituțiile financiare sunt invitate să

[7] Toate articolele menționate se referă la cele din directivă, cu excepția cazului în care se indică altfel.

sesizeze autoritățile de aplicare a legii și alte autorități judiciare cu privire la suspiciunile de fraudă [articolul 15 alineatul (2)]. Sesizarea este deseori punctul de plecare al investigărilor (considerentul 27).

În cele din urmă, articolele 16 și 17 din directivă se referă la **asistența și sprijinul acordate victimelor** și, respectiv, la **prevenție**.

1.2 Scopul și metodologia raportului

Articolul 20 din directivă solicită statelor membre să asigure intrarea în vigoare a actelor cu putere de lege și a actelor administrative necesare pentru a se conforma directivei până la 31 mai 2021 și să informeze Comisia cu privire la aceasta.

Prezentul raport răspunde cerinței prevăzute la articolul 21 din directivă conform căruia Comisia trebuie să prezinte Parlamentului European și Consiliului un raport de evaluare a gradului în care statele membre au luat măsurile necesare pentru a se conforma directivei. Raportul – primul în temeiul articolului 21 – oferă o imagine de ansamblu a principalelor măsuri de transpunere adoptate de statele membre.

Procesul de transpunere de către statele membre a implicat colectarea de informații cu privire la legislația și măsurile administrative relevante, analizarea acestora, elaborarea de noi acte legislative sau – de cele mai multe ori – modificarea celor existente, urmărirea lor până la adoptare și, în final, raportarea acestora către Comisie.

Până la data transpunerii (31 mai 2021), 9 state membre notificaseră Comisiei că finalizaseră pe deplin transpunerea directivei și comunicaseră măsurile lor de transpunere. În iulie 2021, Comisia a inițiat proceduri de constatare a neîndeplinirii obligațiilor pentru necomunicarea măsurilor naționale de transpunere împotriva celor 16 state membre rămase: AT, BE, BG, CY, CZ, EL, ES, HR, IT, LU, LV, MT, PL, PT, RO și SI[8]. În timp ce, de atunci, 15 state membre și-au notificat măsurile de transpunere, la 30 aprilie 2023 procedura de constatare a neîndeplinirii obligațiilor pentru necomunicarea măsurilor naționale de transpunere împotriva BG este încă pendinte[9].

Descrierea și analiza care urmează în cadrul prezentului raport se bazează pe informațiile privind măsurile naționale de transpunere pe care statele membre le-au furnizat până la 31 ianuarie 2023. Notificările primite după data respectivă nu au fost luate în considerare. S-a ținut seama de toate măsurile notificate referitoare la legislația națională, precum și de hotărârile judecătorești și, după caz, de teoria juridică acceptată în comun. În plus, în cursul analizei, Comisia a contactat statele membre în mod direct, după caz, pentru a primi informații suplimentare sau clarificări. Toate informațiile colectate au fost luate în considerare în cadrul analizei.

Dincolo de aspectele identificate în prezentul raport, este posibil să existe noi provocări în ceea ce privește transpunerea și alte dispoziții care nu au fost raportate Comisiei sau evoluții legislative și nelegislative viitoare. Prin urmare, prezentul raport nu împiedică Comisia să

[8] În prezentul document, abrevierile pentru statele membre sunt în conformitate cu: http://publications.europa.eu/code/ro/ro-5000600.htm.

[9] Informații referitoare la deciziile Comisiei privind procedurile de constatare a neîndeplinirii obligațiilor pot fi consultate la adresa: http://ec.europa.eu/atwork/applying-eu-law/infringements-proceedings/infringement_decisions/?lang_code=ro.

evalueze în continuare anumite dispoziții și să continue să sprijine statele membre în transpunerea și punerea în aplicare a directivei.

2. Măsuri de transpunere

2.1 Definiții juridice

Articolul 2 din directivă stabilește definițiile principalilor termeni utilizați, și anume: instrument de plată fără numerar; dispozitiv, obiect sau înregistrare protejat(ă); mijloace digitale de schimb; monedă virtuală; sistem informatic; date informatice; persoană juridică.

În general, statele membre au transpus definițiile bazându-se pe legi anterioare directivei sau adoptate după intrarea în vigoare a acesteia. În unele cazuri, deși nu există dispoziții care să stabilească în mod specific definiții, infracțiunile sunt transpuse prin dispoziții generale ale codului penal care au un domeniu de aplicare mai larg, de exemplu dispoziții privind furtul. Prin urmare, necomunicarea unei transpuneri textuale a definiției nu indică neapărat caracterul incomplet sau neconformitatea.

În plus, mai multe dintre definiții fac trimiteri la definițiile prevăzute în alte directive.

a) Instrumente de plată fără numerar

Evaluarea a evidențiat cel puțin un caz de transpunere incompletă, întrucât definiția stabilită de Decizia-cadru 2001/413/JAI a Consiliului nu fusese actualizată. În consecință, aceasta se referă numai la instrumentele de plată materiale și nu include „un dispozitiv, un obiect sau o înregistrare protejat(ă) [...] sau o combinație a acestora", astfel cum prevede definiția din directivă.

b) Dispozitiv, obiect sau înregistrare protejat(ă)

Mai multe state membre nu au transpus această definiție (BG, CZ, EE, ES, FI, HR, LT, NL, PL, PT, RO, SI). Acest lucru nu este neapărat considerat un caz de neconformitate, întrucât, de regulă, sensul este de la sine înțeles sau poate fi derivat din formularea definiției instrumentului de plată fără numerar. În unele țări, conceptul este explicat în lucrările pregătitoare.

c) Mijloace digitale de plată și monedă virtuală

Aceste două definiții sunt esențiale pentru Directiva 2019/713, al cărei obiectiv principal a fost acela de a aborda faptul că Decizia-cadru 2001/413/JAI nu mai reflectă realitățile actuale și nu mai abordează suficient noile provocări și evoluții tehnologice, cum ar fi monedele virtuale și aplicațiile de plată mobilă, care trebuiau incluse pentru a asigura un răspuns cuprinzător la acest fenomen și pentru a elimina lacunele neintenționate în materie de incriminare.

Principala problemă întâlnită în transpunere este acoperirea monedei virtuale, definită la articolul 2 litera (d) din directivă. Deși moneda electronică este definită în toate statele membre, adesea ca urmare a transpunerii Directivei privind moneda electronică[10], definirea și acoperirea monedei virtuale nu sunt întotdeauna simple.

[10] Directiva 2009/110/CE a Parlamentului European și a Consiliului din 16 septembrie 2009 privind accesul la activitate, desfășurarea și supravegherea prudențială a activității instituțiilor emitente de monedă electronică, de modificare a Directivelor 2005/60/CE și 2006/48/CE și de abrogare a Directivei 2000/46/CE, JO L 267, 10.10.2009.

În HU, moneda virtuală este considerată drept proprietate și element de date electronice și poate face obiectul confiscării bunurilor și sechestrului. În mod similar, în PL, moneda virtuală nu este definită în legislație și există un anumit nivel de incertitudine cu privire la faptul dacă aceasta ar fi acoperită de diferitele infracțiuni relevante pentru transpunerea directivei, deși unii autori consideră că moneda virtuală ar putea intra sub incidența dispozițiilor codului penal care reglementează infracțiunile referitoare la informații, la mediile de stocare a datelor sau la datele informaționale.

Multe state membre au transpus aceste definiții mai degrabă prin norme financiare decât prin legi penale (AT, BE, BG, CY, CZ, DE, EE, EL, ES, HR, HU, LT, LU, LV, SI). Totuși, nu în toate aceste cazuri, există o trimitere la dispozițiile relevante din legislația națională care stabilesc infracțiunile. În cele din urmă, în trei state membre (IT, MT, RO), ambele definiții sunt transpuse în codul penal.

d) Sistem informatic

Articolul 2 litera (e) definește „sistemul informatic" făcând trimitere la articolul 2 litera (a) din Directiva 2013/40/UE. Toate statele membre au transpus definiția în conformitate cu directiva.

e) Date informatice

Datele informatice sunt definite la articolul 2 litera (f) prin trimitere la articolul 2 litera (b) din Directiva 2013/40/UE. Toate statele membre au transpus articolul 2 litera (f) în conformitate cu directiva.

f) Persoană juridică

În sfârșit, articolul 2 litera (g) definește noțiunea de „persoană juridică". Aproape toate statele membre au transpus această noțiune în legislația lor. Singura excepție este SE, care nu definește „persoana juridică". Termenul cel mai apropiat utilizat în transpunere este „întreprindere". Acest termen nu este definit în niciun text juridic și nici în doctrină sau jurisprudență.

2.2 Infracțiuni specifice

a) Utilizarea frauduloasă a instrumentelor de plată fără numerar

Articolul 3 litera (a) din directivă impune statelor membre să ia măsurile necesare pentru a se asigura că utilizarea frauduloasă a unui instrument de plată fără numerar furat sau însușit sau obținut în alt mod în mod ilegal, atunci când este săvârșită cu intenție, se pedepsește ca infracțiune.

25 de state membre au transpus articolul 3 litera (a) din directivă. Dintre cele 25 de țări, 14 au transpus directiva printr-o dispoziție specifică privind utilizarea frauduloasă a instrumentelor de plată fără numerar (AT, CY, ES, FI, HU, IT, LT, MT, NL, PT, RO, SE, SI, SK). Celelalte state membre au făcut referire la infracțiuni mai generale, cum ar fi frauda și contrafacerea calculatoarelor, sau la fraude legate de mijloace de plată care nu se limitează la instrumente de plată fără numerar (BE, BG, CZ, DE, EE, EL, FR, HR, LU, LV, PL, SE, SK).

Legislația HR nu se referă la utilizarea instrumentelor de plată furate sau însușite în alt mod ilegal; dispoziția de transpunere din HU se referă numai la instrumentele de plată electronice fără numerar.

În conformitate cu articolul 3 litera (b) din directivă, statele membre iau măsurile necesare pentru a se asigura că utilizarea frauduloasă a unui instrument de plată fără numerar contrafăcut sau falsificat, atunci când este comisă intenționat, se pedepsește ca infracțiune.

În general, articolul 3 litera (b) a fost transpus integral.

Pentru a transpune directiva, 15 state membre fac trimitere la dispozițiile naționale privind instrumentele de plată fără numerar (AT, CY, DE, EE, ES, FI, HR, HU, IT, LT, MT, NL, PT, RO, SI), în timp ce legislația națională de transpunere din zece state membre acoperă infracțiuni mai generale, cum ar fi furtul sau frauda sau infracțiuni legate de instrumente de plată, dar nu în mod specific instrumente fără numerar (BE, BG, CZ, EL, FR, LU, LV, PL, SE, SK).

b) Infracțiuni legate de utilizarea frauduloasă a instrumentelor de plată fără numerar materiale

Articolul 4 din directivă impune statelor membre să ia măsurile necesare pentru a se asigura că actele săvârșite cu intenție enumerate în alineatele sale se pedepsesc ca infracțiuni. Paragrafele includ furtul sau însușirea în alt mod ilegal a unui instrument de plată fără numerar material (a); contrafacerea sau falsificarea frauduloasă a unui instrument de plată fără numerar material (b); posesia în vederea utilizării frauduloase a unui instrument de plată fără numerar material, furat sau însușit pe alte căi ilegale, sau contrafăcut sau falsificat (c); achiziția în folosul propriu sau al unei alte persoane, inclusiv primirea, însușirea, cumpărarea, transferul, importul, exportul, vânzarea, transportul sau distribuirea în vederea utilizării frauduloase a unui instrument de plată fără numerar material, furat, contrafăcut sau falsificat (d).

Deși articolul 4 pare, în cea mai mare parte, să fi fost transpus într-un mod mai mult sau mai puțin textual, în câteva cazuri transpunerea la nivel național ridică semne de întrebare în ceea ce privește actele specifice de achiziție în folosul propriu sau al unei alte persoane a unui instrument de plată material fără numerar furat, contrafăcut sau falsificat în scopul utilizării frauduloase.

c) Infracțiuni legate de utilizarea frauduloasă a instrumentelor de plată fără numerar nemateriale

Articolul 5 din directivă incriminează comportamentele legate de utilizarea frauduloasă a instrumentelor de plată fără numerar nemateriale. În urma analizei, s-a constatat că acest articol nu pare să fi creat dificultăți în ceea ce privește transpunerea. În majoritatea cazurilor, dispoziția națională se aplică atât instrumentelor de plată materiale, cât și instrumentelor de plată nemateriale. Aproximativ jumătate dintre statele membre au transpus articolul 5 din directivă printr-o dispoziție mai generală (BE, BG, DE, EE, FI, HR, FR, LV, PL, SE, SK), iar mai mult de jumătate dintre acestea l-au transpus printr-o dispoziție referitoare în mod specific la utilizarea frauduloasă a instrumentelor de plată fără numerar (AT, CY, CZ, EL, ES, HU, IT, LT, LU, NL, PT, RO, SI).

d) Frauda legată de sistemele informatice

Articolul 6 din directivă prevede obligația statelor membre de a asigura efectuarea sau provocarea efectuării unui transfer de bani, de valoare monetară sau de monedă virtuală având drept efect cauzarea unui prejudiciu patrimonial unei alte persoane, cu scopul de a obține un profit ilegal pentru autor sau pentru un terț, se pedepsește ca infracțiune atunci când este săvârșită cu intenție prin perturbarea sau afectarea fără drept a funcționării unui sistem informatic [articolul 6 litera (a)]; sau introducerea, modificarea, ștergerea, transmiterea sau suprimarea fără drept a datelor informatice [articolul 6 litera (b)]. Toate statele membre au transpus articolul 6.

e) Instrumente utilizate pentru săvârșirea infracțiunilor

Articolul 7 din directivă prevede obligația statelor membre de a lua măsurile necesare pentru a se asigura că producerea, achiziționarea în folos propriu sau al unei alte persoane sau punerea la dispoziție a unui dispozitiv sau a unui instrument, a unor date informatice sau a oricăror alte mijloace concepute în principal sau adaptate special în scopul săvârșirii uneia dintre infracțiunile menționate la articolul 4 literele (a) și (b), la articolul 5 literele (a) și (b) sau la articolul 6, cel puțin atunci când sunt săvârșite cu intenția ca aceste mijloace să fie folosite, se pedepsește ca infracțiune.

Marea majoritate a statelor membre au transpus articolul 7 din directivă (AT, CY, CZ, DE, EE, ES, FI, FR, HR, IT, LT, LV, NL, RO, SE, SI, SK).

Șase țări au transpus articolul 7 din directivă prin dispoziții care se referă la dispoziții mai ample, fie cu privire la infracțiuni generale, cum ar fi furtul, fie cu privire la instrumente financiare și mijloace de plată (BG, FI, FR, LV, SE, SK). 17 țări l-au transpus printr-o dispoziție specifică privind instrumentele utilizate pentru comiterea diferitelor infracțiuni prevăzute în directivă legate de instrumentele de plată fără numerar materiale sau nemateriale (AT, CY, CZ, DE, EE, EL, ES, HR, HU, IT, LT, LU, MT, NL, PL, RO, SI).

Cinci state membre par să se fi confruntat cu dificultăți în ceea ce privește transpunerea (BE, BG, HU, PL, PT).

2.3 Norme generale pentru infracțiunile în cauză

a) Instigarea, complicitatea și tentativa

În temeiul articolului 8 alineatul (1) din directivă, statele membre trebuie să se asigure că instigarea sau complicitatea la una din infracțiunile menționate la articolele 3-7 se pedepsește ca infracțiune.

Toate statele membre au transpus această dispoziție. Marea majoritate a statelor membre au transpus directiva printr-un articol preexistent privind instigarea și complicitatea în general (AT, BE, BG, CZ, DE, EE, EL, ES, FI, FR, HR, HU, IT, LT, LU, LV, NL, PL, PT, RO, SE, SI, SK). Cu toate acestea, două state membre au decis să adopte o nouă dispoziție, care se aplică numai în contextul infracțiunilor prevăzute de directivă (CY, MT).

Articolul 8 alineatul (2) prima teză din directivă prevede obligația statelor membre de a se asigura că tentativa de a săvârși una dintre infracțiunile menționate la articolul 3, la articolul 4 litera (a), (b) sau (d), la articolul 5 litera (a) sau (b) sau la articolul 6 se pedepsește ca infracțiune. Toate statele membre par să fi transpus această dispoziție în mod complet, cu excepția BE, LU și SI.

Și în acest caz, majoritatea statelor membre au transpus directiva printr-o dispoziție preexistentă care se aplică tentativei în general (AT, BG, CZ, EE, EL, ES, FR, HR, HU, IT, LT, LV, NL, PL, PT, SE, SK). Celelalte au inclus-o într-o măsură specială de transpunere (CY, DE, FI, MT, RO).

Statele membre trebuie, de asemenea, să se asigure că tentativa de achiziționare frauduloasă a unui instrument de plată fără numerar nematerial obținut pe căi ilegale, contrafăcut sau falsificat în folosul propriu sau al unei alte persoane [articolul 5 litera d)] se pedepsește ca infracțiune [articolul 8 alineatul (2) a doua teză].

Evaluarea a arătat că incriminarea tentativei poate face obiectul unor limitări care nu sunt prevăzute în directivă în două state membre (HR, SI).

Toate celelalte state membre au transpus dispozițiile relevante ale directivei. Acestea au făcut acest lucru fie printr-un articol privind tentativa în general (AT, BE, BG, CZ, IT, EE, EL, ES, FR, HU, LT, LU, LV, NL, PL, PT, SE, SK), fie printr-o măsură specială de transpunere (CY, DE, FI, MT, RO).

b) Pedepse

Articolul 9 prevede că infracțiunile prevăzute la articolele 3-8 sunt pasibile de pedepse eficace, proporționale și disuasive și prevede o durată maximă a pedepsei cu închisoarea pentru diferitele infracțiuni.

Deși statele membre au transpus, în general, articolul 9 din directivă, evaluarea a identificat posibile probleme legate de domeniul de aplicare al definiției referitoare la articolul 9 alineatul (2) în HR și la articolul 9 alineatul (6) în BE, CZ, HR și HU.

Compararea sancțiunilor stabilite de statele membre pentru diferitele infracțiuni este complicată, deoarece infracțiunile sunt reglementate atât de dispoziții generale, cât și de dispoziții specifice. Atunci când au transpus directiva prin dispoziții privind infracțiunile generale, statele membre s-au bazat pe mai multe dispoziții naționale pentru a incrimina una dintre faptele interzise de directivă. Acest lucru conduce la mai multe pedepse maxime aplicabile acestei infracțiuni specifice și implică faptul că sancțiunea maximă efectivă ar depinde de fiecare caz în parte, de abordarea adoptată de instanțe și de normele naționale privind sancțiunile paralele. De exemplu, în PL, regula este că o faptă nu poate constitui decât o singură infracțiune. În cazul în care un comportament prezintă caracteristici a două sau mai multe dispoziții de drept penal, instanța trebuie să aleagă o infracțiune specifică. În schimb, în BG, în cazurile în care partea specială din codul penal prevede aplicarea concomitentă a două sau mai multe pedepse pentru o anumită infracțiune, instanța stabilește întinderea fiecărei pedepse, astfel încât suma acestora să fie conformă cu obiectivele generale ale pedepsei.

În plus, dispozițiile pot conține circumstanțe agravante care pot ridica plafonul și pot conduce la înăsprirea sancțiunilor. Prin urmare, pedeapsa maximă depinde de modul în care este săvârșită infracțiunea. De exemplu, dispoziția generală privind deturnarea în HR prevede o pedeapsă maximă cu închisoarea de cinci ani. Cu toate acestea, în cazul în care autorul infracțiunii utilizează forța, pedeapsa maximă este de 10 ani, iar în cazul în care acțiunea a avut ca rezultat un câștig material substanțial, infractorul este pasibil de o pedeapsă cu închisoarea de până la 12 ani. În DE, falsificarea instrumentelor de plată fără numerar materiale se pedepsește cu o pedeapsă maximă de cinci ani de închisoare. Cu toate acestea, în cazul în care autorul infracțiunii a acționat în scop comercial, pedeapsa va fi de maximum 10 ani.

Evaluarea a arătat, de asemenea, că, în majoritatea cazurilor, pragurile prevăzute în legislația internă sunt mai stricte decât cele stabilite de directivă. Diferența poate fi semnificativă: falsificarea banilor se pedepsește cu până la 15 ani în BG și LU și cu până la 25 de ani în PL. Numai două state membre prevăd pedepse maxime identice cu cele prevăzute de directivă (sau foarte apropiate de acestea) (AT, MT).

c) Răspunderea persoanelor juridice

Evaluarea a arătat că 16 state membre au transpus articolul 10 din directivă printr-o dispoziție generală deja existentă din codul penal (AT, CZ, BE, BG, DE, EE, ES, FR, HR, HU, LU, LV, NL, PT, RO, SE), în timp ce nouă state membre l-au transpus printr-o lege privind în mod specific răspunderea persoanelor juridice în contextul directivei (CY, EL, FI, IT, LT, MT, PL, SI, SK).

d) Sancțiuni aplicabile persoanelor juridice

Articolul 11 din directivă prevede obligația statelor membre de a stabili sancțiuni eficace, proporționale și disuasive sub formă de amenzi penale sau de altă natură și pentru persoanele juridice. Toate statele membre au prevăzut astfel de sancțiuni.

Articolul 11 prevede posibilitatea ca statele membre să includă diferite sancțiuni specifice pentru persoanele juridice, cum ar fi excluderea de la avantajele publice sau lichidarea judiciară. Șase state membre nu au utilizat deloc opțiunea prevăzută la articolul 11 din directivă (AT, BG, EE, FI, NL, SE). Celelalte 19 țări au transpus articolul 11 fie integral, fie parțial (BE, CY, CZ, DE, EL, ES, FR, HR, HU, IT, LT, LU, LV, MT, PL, PT, RO, SI, SK).

e) Competență

Acest articol, care obligă statele membre să își stabilească competența pentru infracțiunile săvârșite pe teritoriul lor sau la nivel național, este transpus în dispozițiile generale ale codului penal național sau ale codului de procedură penală în toate statele membre. Prin urmare, principiul teritorialității și principiul cetățeniei active au aplicabilitate generală, nefiind specifice infracțiunilor reglementate de prezenta directivă. În plus, articolul 12 fost transpus, de asemenea, de CY în Legea națională privind combaterea fraudei și a contrafacerii mijloacelor de plată fără numerar și de PT în Legea privind criminalitatea informatică.

Toate statele membre au transpus articolul 12 alineatul (1) literele (a) și (b).

Articolul 12 alineatul (3) permite statelor membre să își stabilească competența cu privire la o infracțiune menționată la articolele 3-8 din directivă, săvârșită în afara teritoriului lor, în cazul în care, printre altele, (a) infracțiunea este săvârșită de o persoană care își are reședința obișnuită pe teritoriul lor; (b) infracțiunea a fost săvârșită în interesul unei persoane juridice stabilite pe teritoriul lor; sau (c) infracțiunea este săvârșită împotriva unuia dintre cetățenii săi sau împotriva unei persoane care are reședința obișnuită pe teritoriul lor. Paisprezece state membre (BE, CY, CZ, DE, EL, ES, FI, HR, LT, LV, MT, NL, SE, SK) au utilizat opțiunea prevăzută la articolul 12 alineatul (3) litera (a); 12 state membre (BE, CY, CZ, EL, FI, LV, MT, NL, PL, PT, SI, SK) au transpus articolul 12 alineatul (3) litera (b); și 16 state membre (AT, BG, CY, CZ, DE, EE, EL, FI, FR, HR, HU, LV, MT, RO, SE, SI) și-au extins competența în conformitate cu articolul 12 alineatul (3) litera (c). În ceea ce privește litera (c), în BG, DE, EE, HU, RO și SI s-a stabilit competența pentru o infracțiune săvârșită în afara teritoriului lor în cazul în care infracțiunea este săvârșită (numai) împotriva unuia dintre resortisanții lor – omițând astfel reședința obișnuită. AT prevede urmărirea penală de către sistemul austriac de justiție penală pentru infracțiuni săvârșite în străinătate în cazul în care autorul și victima sunt austrieci. CY, CZ, EL, FI, LV și MT au făcut uz de toate cele trei dispoziții opționale prevăzute la articolul 12 alineatul (3).

2.4 Aspecte operaționale

a) Eficacitatea investigațiilor și cooperare

În toate statele membre, instrumentele de investigație pentru anchetarea și urmărirea penală a infracțiunilor menționate la articolele 3-8 nu sunt incluse în mod explicit în legislația de transpunere a directivei, ci mai degrabă în legislația mai generală, cum ar fi codurile de procedură penală. De regulă, posibilitatea de a utiliza un instrument de investigație într-un anumit caz este legată de sancțiunea pentru infracțiunea în cauză; astfel, după cum s-a menționat deja în dispoziția directivei, instrumentele de investigație utilizate în combaterea criminalității organizate sau în alte cazuri de forme grave de criminalitate vor fi, de asemenea, disponibile pentru investigarea și urmărirea penală a infracțiunilor prevăzute în prezenta directivă. Caracterul excepțional al unor instrumente de investigație și necesitatea proporționalității cu infracțiunea sunt cel mai adesea incluse în dispozițiile legale relevante și/sau în Constituție.

Informațiile privind infracțiunile menționate la articolele 3-8 ar trebui să parvină fără întârzieri nejustificate autorităților care investighează sau urmăresc penal aceste infracțiuni, în conformitate cu articolul 13 alineatul (2) din directivă. Cu alte cuvinte, autoritățile de aplicare a legii și alte autorități competente ar trebui să aibă acces în timp util la informațiile relevante pentru investigarea și urmărirea penală a infracțiunilor menționate în prezenta directivă (considerentul 22). Codul de procedură penală prevede adesea diverse sisteme de raportare, astfel încât infracțiunile (în sensul articolelor 3-8 din directivă) să poată fi raportate în mod eficient și rapid. Aceste sisteme de raportare includ: obligația de raportare a organismelor și autorităților publice; un sistem de avertizare în interes public; o procedură de depunere a plângerilor; o obligație a furnizorilor de servicii de plată de a raporta incidentele operaționale sau de securitate grave; și un drept al persoanelor fizice de a raporta incidentele. În plus, unele legi mai specifice pot asigura faptul că rapoartele privind incidentele de securitate (inclusiv rapoartele privind infracțiuni grave, cum ar fi achiziționarea neautorizată, falsificarea și modificarea unui mijloc de plată) sunt raportate autorităților competente cât mai curând posibil. Astfel de legi au fost raportate de AT, CZ, LT, FI, MT și PT.

Condiția ca informațiile transmise să „parvin[ă] fără întârzieri nejustificate autorităților [competente]” nu este, de cele mai multe ori, transpusă în mod explicit.

b) Schimbul de informații

Schimbul de informații între autoritățile naționale de aplicare a legii în vederea investigării și a urmării penale a infracțiunilor, inclusiv a celor menționate la articolele 3-8 din directivă, poate fi facilitat prin intermediul punctelor de contact operaționale (considerentul 26). Articolul 14 alineatul (1) prima teză din directivă garantează faptul că statele membre stabilesc într-adevăr aceste puncte de contact și că acestea sunt disponibile 24 de ore pe zi, șapte zile pe săptămână. În plus, a doua teză obligă statele membre să instituie proceduri pentru a trata cu promptitudine cererile urgente de asistență și să ofere un răspuns în termen de opt ore, indicând cel puțin dacă cererea va primi un răspuns, precum și forma unui astfel de răspuns și termenul estimat pentru transmiterea acestuia.

Următoarele state membre au decis să utilizeze un punct de contact operațional existent în scopurile descrise în prezenta directivă: AT, BE, CY, EE, EL, ES, FR, HU, IT, LT, LV, NL, PL, PT, SE.

Tabelul 1 oferă o imagine de ansamblu a punctelor de contact stabilite. În BG, CZ, LU, SI, HR, nu au fost identificate puncte de contact.

Tabelul 1 Puncte de contact operaționale

SM	Punct de contact	SM	Punct de contact
AT	Biroul Federal de Poliție Judiciară	**EE**	Ministerul Justiției
BE	Direcția Informații Polițienești Operaționale	**FI**	Biroul național de date operative
BG	N/A	**FR**	Divizia pentru relații internaționale a Direcției centrale a poliției judiciare
CY	Poliția cipriotă	**HR**	N/A
CZ	N/A	**HU**	Centrul de Cooperare Penală Internațională (NEBEK)
DE	16 birouri naționale de poliție judiciară și un birou federal de poliție judiciară – Puncte de contact centrale privind criminalitatea informatică	**MT**	Forța de poliție din Malta
EL	Poliția elenă (Divizia de cooperare polițienească internațională)	**ES**	Celula de coordonare în situații de urgență
IT	Camera de operațiuni internaționale a Serviciului de Cooperare Polițienească Internațională	**NL**	Centrul Național de Asistență Juridică Internațională (LIRC)
LT	Divizia a 2-a a Consiliului de Administrare a Forțelor din cadrul Departamentului de Poliție al Ministerului de Interne al Republicii Lituania și Consiliul pentru relații internaționale al Biroului Poliției Judiciare din Lituania	**PL**	Inspectoratului General al Poliției
LV	Poliția națională	**PT**	Poliția judiciară
RO	Secția de urmărire penală și criminalistică a Parchetului General	**SE**	Autoritatea polițienească
SI	N/A	**SK**	Biroul Poliției Judiciare din cadrul Prezidiului forțelor de poliție din Republica Slovacă

Articolul 14 alineatul (1) a doua teză din directivă a fost pus în aplicare în câteva state membre. În BE, BG, CZ, LV, RO, FR, HR, LU, NL, PL, SE și SK nu au fost găsite informații privind procedurile care se aplică cererilor urgente.

c) Semnalarea infracțiunilor

Statele membre sunt, de asemenea, obligate să pună la dispoziție canale adecvate de semnalare. Astfel de canale de semnalare a suspiciunilor de fraudă sau, la un nivel mai general, de semnalare a oricăror posibile infracțiuni pot fi stabilite prin acte legislative. Adesea, statele membre au stabilit semnalarea unei infracțiuni ca o obligație pentru anumite categorii de persoane (fizice și juridice) [în mare măsură în conformitate cu articolul 15 alineatul (2)], în timp ce victimelor și altor „persoane prezente” li se oferă posibilitatea (dar nu și obligația) de semnalare. Aceste dispoziții legale sunt, de obicei, completate de punerea în aplicare practică.

În toate statele membre, se pot prezenta rapoarte scrise sau orale poliției și/sau sistemului judiciar. În plus, unele state membre au pus la dispoziție canale de semnalare suplimentare:

Legea federală din AT prevede diverse sisteme de semnalare, astfel încât infracțiunile în sensul articolelor 3-8 din directivă să poată fi semnalate în mod eficient și rapid: 1) obligația de raportare a organismelor și autorităților publice; 2) sistemul de avertizare în interes public din cadrul Parchetului pentru afaceri economice și corupție; 3) sistemul de avertizare în interes public al Autorității pentru Piața Financiară; și 4) obligația furnizorilor de servicii de plată de a raporta incidentele operaționale sau de securitate grave. Un birou specific de sesizare pentru criminalitatea informatică a fost înființat în cadrul Biroului Federal al Poliției Judiciare. În plus, Ministerul Federal de Interne cooperează cu Camera economică federală. Prin urmare, au loc diverse corespondențe și campanii, care motivează și încurajează publicul să raporteze încălcări relevante ale legii.

În BE, Ministerul Economiei deține un punct unic de contact pentru victimele fraudelor, practicilor de scam, escrocheriilor și înșelătoriilor. În plus, Autoritatea pentru Servicii Financiare și Piețe a instituit și a pus la dispoziție în mod legal un canal de avertizare în interes public pentru toate plângerile legate de produsele și serviciile de credit sau de investiții.

În CY, poliția cipriotă, împreună cu Banca Centrală a Ciprului și cu autoritatea națională pentru securitatea rețelelor și a sistemelor informatice, sunt desemnate în mod oficial, printr-o măsură legislativă, ca autorități naționale competente responsabile cu instituirea unor canale adecvate de semnalare și comunicare.

Dreptul penal din CZ prevede obligația de semnalare a autorităților de stat.

În DE, entitățile obligate trebuie să semnaleze tranzacțiile suspecte, fără întârzieri nejustificate. În plus, au fost adoptate măsuri fără caracter legislativ la nivel federal, cum ar fi un parteneriat public-privat instituționalizat în scopul depistării, prevenirii, investigării sau urmăririi penale a infracțiunilor menționate la articolele 3-8 din directivă, precum și o platformă pentru schimbul de informații.

În EL, pe lângă canalele generale de semnalare, guvernul elen a creat un serviciu de stat online prin care cetățenii pot depune în mod direct plângeri privind infracțiuni comise online. În plus, instituțiile de credit și alți furnizori de servicii de plată trebuie să semnaleze Băncii Greciei (care are competențe în ceea ce privește astfel de plângeri) orice incidență a fraudei imediat ce o întâlnesc.

În ES, pe lângă canalele generale de semnalare a infracțiunilor, Banca Spaniei pune la dispoziție un canal de semnalare în colaborare cu Institutul Național de Securitate Cibernetică.

Legislația italiană asigură promptitudinea comunicării către procuror de către poliția judiciară a informațiilor privind o infracțiune, dobândite din proprie inițiativă sau în urma unei plângeri sau a unui proces. Schimbul de informații este încurajat, de asemenea, prin intermediul platformelor digitale.

LT dispune de mai multe canale pentru a semnala infracțiunile menționate la articolele 3-8 din directivă, prin intermediul unei pagini de internet (portalul e-Poliție), al numărului de telefon de urgență general 112, personal, prin e-mail, prin mesaj text și prin aplicația mobilă e-Police, precum și prin alte mijloace automate. Furnizorii de servicii de plată, instituțiile financiare și alte entități obligate, Banca Lituaniei și Serviciul de investigare a infracțiunilor financiare au obligația de a semnala autorităților competente de aplicare a legii suspiciuni rezonabile de acțiuni penale și/sau alte acțiuni ilegale.

În LU, este disponibil un site internet care explică modul de semnalare a fraudelor. Comisia pentru controlul sectorului financiar a stabilit orientări pentru detectarea fraudei financiare, dar solicită, de asemenea, ca toate unitățile aflate sub supravegherea sa să semnaleze cât mai curând posibil orice fraudă și orice incident cauzat de atacuri informatice externe.

În RO, există o obligație de raportare pentru funcționarii publici și persoanele care dețin funcții de conducere în cadrul autorităților publice, persoanele care prestează servicii de interes public și persoanele care acționează în cadrul organismelor de control și supraveghere.

În SI există obligația de a raporta o infracțiune pentru toate autoritățile și organizațiile de stat cu autoritate publică.

Platforma Perceval din FR, instituită printr-un act juridic, permite victimelor să raporteze cu privire la fraudarea și contrafacerea cardurilor bancare. Există o platformă similară pentru raportare cu privire la criminalitatea cibernetică. În plus, sancțiunile se aplică oricărei persoane (fizice sau juridice) care nu împiedică prin acțiunea sa imediată o infracțiune, conducând astfel la o obligație generală de raportare.

În HU, obligația de a raporta o infracțiune este stabilită numai pentru membrii autorității, funcționarii publici și organismele profesionale statutare. Banca Națională a Ungariei încurajează instituțiile financiare pe site-ul său internet, sub forma unui aviz, să raporteze suspiciunile de fraudă.

În MT, punctul național de contact încurajează raportarea, în special de către instituțiile financiare, a suspiciunilor de fraudă și de contrafacere a mijloacelor de plată fără numerar.

Pe lângă canalul de raportare pentru avertizare în interes public instituit în mod legal în PT, există un sistem de raportare a cazurilor de criminalitate informatică disponibil printr-un simplu clic, unde se poate accesa un link care deschide instantaneu un e-mail adresat autorităților competente.

În SE, anumite tipuri de infracțiuni, cum ar fi frauda cu cărți de credit, pot fi, de asemenea, raportate prin intermediul serviciului electronic al autorității polițienești. De asemenea, actorii din sectorul bancar și al activităților de finanțare sunt obligați să raporteze autorității polițienești activitățile suspecte legate de posibile cazuri de spălare de bani sau de finanțare a terorismului sau de bunuri care provin în alt mod dintr-o infracțiune. În plus, se menține un dialog permanent între operațiunile bancare și financiare și Centrul Național Antifraudă al Autorității de Poliție.

Dispozițiile legale din SK stabilesc o cerință (și proceduri) pentru autoritățile publice și alte persoane juridice de a semnala de îndată infracțiunile autorităților de aplicare a legii. Există, de asemenea, obligații de raportare referitoare la spălarea banilor în cazul persoanelor obligate și, în special, al băncilor.

Ca alternativă, în NL și PL au avut loc acțiuni fără caracter legislativ de punere în aplicare a articolului 15 din directivă. Liniile serviciului de poliție neerlandez și site-ul web al poliției oferă un canal adecvat pentru semnalarea către autorități a fraudelor care implică mijloace de plată fără numerar. În plus, guvernul neerlandez s-a angajat să încurajeze instituțiile financiare și alte persoane juridice să semnaleze orice suspiciune de fraudă. Efortul este evident, de exemplu, prin existența unui ghișeu pentru fraudă financiară, instituit în toate unitățile de poliție din Țările de Jos. De asemenea, patru bănci importante și emitenți de carduri ICS au semnat un pact cu poliția pentru a combate în comun frauda (bancară) și phishingul. În PL, rapoartele privind infracțiunile sunt acceptate 24 de ore pe zi, șapte zile pe săptămână de către toate unitățile de poliție. În plus, având în vedere natura infracțiunilor comise prin utilizarea tehnologiilor informatice, este posibil ca acestea să fie contactate direct cu o unitate organizațională specializată a inspectoratului general de poliție. În plus, pentru a asigura o cooperare cât mai rapidă cu sectorul bancar, a fost instituit un canal de cooperare între Biroul pentru combaterea criminalității informatice de la Inspectoratul general al poliției și Centrul de securitate bancară al Asociației băncilor poloneze.

Articolul 15 alineatul (2) din directivă nu a fost transpus în BG, EE, HR.

2.5 Sprijin pentru victime și prevenție

a) Asistență și sprijin acordate victimelor

Asistența și sprijinul acordate persoanelor fizice și juridice ale căror date cu caracter personal au fost utilizate în mod abuziv sunt asigurate prin articolul 16 alineatul (1) din directivă. Măsurile ar trebui să includă: a) oferirea de informații și consiliere specifice privind protecția împotriva consecințelor negative ale unor astfel de infracțiuni și b) furnizarea unei liste de instituții specializate care se ocupă cu diferite aspecte ale infracțiunilor legate de identitate și cu sprijinirea victimelor.

În aceeași ordine de idei, persoanele juridice care sunt victime ale infracțiunilor menționate la articolele 3-8 din prezenta directivă ar trebui să aibă acces la informații privind a) procedurile de formulare a plângerilor, b) dreptul de a primi informații cu privire la cauză, c) procedurile disponibile pentru formularea plângerilor, dacă autoritatea competentă nu respectă drepturile victimei în cursul procedurilor penale și d) datele de contact pentru comunicările privind cauza lor [articolul 16 alineatul (3) din directivă].

Codul de procedură penală din majoritatea statelor membre conține reglementări privind victimele și drepturile acestora, inclusiv unele dispoziții specifice privind drepturile victimelor la informare și asistență în cursul procedurilor, dreptul la consiliere și dreptul de a depune o plângere. O lege specifică de transpunere a directivei completează adesea ceea ce a fost deja prevăzut în codul de procedură penală. De regulă, persoanele juridice sunt tratate în dispoziții juridice separate în cadrul codului de procedură penală sau în altă parte. În plus, sunt disponibile diverse campanii de informare, broșuri, site-uri web dedicate, circulare etc. pentru a oferi asistență și sprijin victimelor infracțiunilor menționate la articolele 3-8 din directivă. Acesta este cazul AT, BE [în ceea ce privește articolul 16 alineatul (1)], CY, CZ, DE, IT, LT, LU [în ceea ce privește articolul 16 alineatul (1)], LV [în ceea ce privește articolul 16 alineatul (3)], RO, SI [în ceea ce privește articolul 16 alineatul (3)], EE, FI [în ceea ce privește articolul 16 alineatul (1)], FR [în ceea ce privește articolul 16 alineatul (1)], HR, HU, NL, PL [în ceea ce privește articolul 16 alineatul (3)], PT, SE și SK. Articolul 16 alineatul (1) și/sau articolul 16 alineatul (3) din directivă nu au fost transpuse textual sau aproape textual de niciun stat membru, cu excepția MT.

Lista instituțiilor de consiliere acreditate care oferă sprijin victimelor, astfel cum se menționează la articolul 16 alineatul (1) litera (b) din directivă, este în mod normal disponibilă online și, prin urmare, este pusă în practică.

b) Prevenție

Articolul 17 privind prevenția impune statelor membre să ia măsuri adecvate, cum ar fi campanii de informare și de sensibilizare și programe de cercetare și de educație. Această secțiune se bazează pe o evaluare a informațiilor notificate Comisiei de către statele membre, precum și pe o cercetare a serviciilor de internet cu sursă deschisă pentru a explora existența unor măsuri de prevenție. Astfel cum se descrie în tabelul 2 de mai jos, atunci când au fost identificate acțiuni de prevenție, acestea se referă în principal la criminalitatea informatică și la frauda online. Cu toate acestea, în unele țări, informațiile privind prevenirea fraudei sunt, de asemenea, furnizate, de obicei, de poliție.

Tabelul 2 Acțiuni de prevenție

SM	Acțiuni
AT	Poliția federală furnizează în mod regulat informații pe site-ul său internet și pe rețelele sociale cu privire la modalitățile de a se proteja împotriva fraudei. Cooperarea cu părțile interesate, cum ar fi Camera de Comerț, este sprijinită și pusă în aplicare în cadrul proiectelor privind comerțul electronic.
BE	Diferite site-uri web cu materiale de consiliere/sensibilizare, cum ar fi cele gestionate de Centrul pentru Securitate Cibernetică din Belgia (CCB). Exemple de cooperare cu părțile interesate ar putea fi identificate prin căutare pe internet, de exemplu organizația care reprezintă sectorul financiar a cooperat cu Parchetul din Bruxelles (*parquet*) pentru elaborarea de materiale de sensibilizare.
BG	În 2021, în Bulgaria a început o campanie de combatere a fenomenului reprezentat de intermediarii pentru transferul de bani obținuți ilegal, condusă de Asociația Băncilor și desfășurată împreună cu Direcția Generală „Combaterea criminalității organizate” și cu parchetul. Direcția Generală a lansat, de asemenea, o campanie privind phishingul.
CY	Subdiviziunea de combatere a criminalității informatice din cadrul poliției pune la dispoziție pe site-ul său internet informații și recomandări cu privire la aspecte precum frauda digitală, precum și informații cu privire la evenimentele viitoare, de exemplu campanii de sensibilizare. Un exemplu în acest sens este campania de informare privind securitatea informațiilor desfășurată de poliție, băncile centrale, Asociația Băncilor și Autoritatea pentru Securitate Digitală.
DE	Poliția federală (BKA) oferă pe site-ul său o prezentare generală a măsurilor care vizează parteneriatul public-privat instituționalizat în scopul detectării, prevenirii, investigării sau urmăririi penale a infracțiunilor reglementate de directivă, de exemplu parteneriatul dintre Oficiul Federal al Poliției Judiciare (BKA), Oficiul Federal pentru Securitatea Informațiilor (BSI) și „Centrul german de competențe de combatere a criminalității informatice e.V.” (G4C), o asociație de instituții financiare și întreprinderi din sectorul securității informatice. BKA a lansat, de asemenea, Conferința

	privind criminalitatea informatică C³, o platformă pentru schimburi între autorități, mediul de afaceri, științific și politic. G4C elaborează, de asemenea, broșuri informative și cursuri de formare. În cele din urmă, BKA participă, de asemenea, la măsuri de prevenție în domeniul criminalității informatice la nivelul landurilor și, la nivel național; BKA este, de asemenea, interconectată cu alte autorități și organizații polițienești și non-polițienești (părți interesate) și își intensifică cooperarea, în special în ceea ce privește subiectele de interes.
FR	Ministerul de Interne publică informații privind prevenția cibernetică. Platformele disponibile pentru semnalarea formelor de criminalitate informatică includ, de asemenea, mesaje de prevenție, precum și Serviciul național de informare și comunicare al Poliției Naționale (SICoP). Alte exemple includ orientările emise de Banca Franței sau ghidul privind prevenirea fraudei publicat de Grupul operativ național de lupta împotriva fraudei, care grupează diferite autorități administrative și de aplicare a legii.
EL	Departamentul pentru criminalitatea informatică și Inspectoratul general al poliției sunt foarte active în ceea ce privește informarea publicului, sensibilizarea și reducerea riscului de a deveni victime ale fraudei, prin campanii TV, discursuri educaționale și informații online.
ES	Institutul Național de Securitate Cibernetică și Agenția fiscală din Spania furnizează pe site-urile lor informații relevante pentru a preveni fenomene de tip phishing, ransomware etc. în mediile de afaceri.
HR	Ministerul de Interne furnizează informații online cu privire la fraudele de pe internet și gestionează un canal YouTube dedicat fraudei și securității informatice, care conține materiale video despre practicile de scam.
IT	Departamentul de Trezorerie, care are sarcina de a preveni fraudele legate de mijloacele de plată, promovează deja o serie de inițiative la nivel local, în colaborare cu administrațiile locale și cu mediul universitar, organizând seminare și ateliere destinate categoriilor implicate în falsificarea de monede, inclusiv cetățenilor.
LT	Informații privind prevenția pot fi găsite pe site-ul Autorității de reglementare a comunicațiilor în legătură cu frauda online și pe site-ul poliției privind cele mai frecvente tipuri de fraudă cibernetică. În plus, unul dintre obiectivele Strategiei naționale privind criminalitatea informatică este de a consolida prevenția și controlul criminalității informatice, în special prin dezvoltarea unei cooperări eficace între autoritățile de aplicare a legii și alte părți interesate.
LV	Comisia pentru piețele financiare și de capital a elaborat diverse instrumente pe internet pentru a furniza informații și orientări privind securitatea financiară și aspectele legate de fraudă. În plus, au fost organizate diverse campanii în cooperare cu poliția de stat și cu Centrul pentru protecția drepturilor consumatorilor.
NL	Există măsuri, cum ar fi „Fraudehelpdesk” (linia telefonică de asistență antifraudă), o organizație subvenționată de guvernul neerlandez. În cazul în care pot fi raportate acțiuni frauduloase, serviciul Fraudehelpdesk face parte din SAFECIN stichting [Fundația pentru combaterea criminalității financiare și economice în Țările de Jos (SAFECIN)], o fundație cu implicare guvernamentală.
SE	Se menține un dialog permanent între operațiunile bancare și financiare și Centrul Național Antifraudă al Autorității de Poliție, NBC. În plus, NBC colaborează, de asemenea, în scopul prevenirii criminalității, de exemplu cu actorii din domeniul comerțului electronic. Importanța raportării fraudelor către poliție este subliniată în cadrul acestor contacte.

În zece state membre (CZ, EE, FI, HU, MT, PL, PT, RO, SI, SK), nu au fost găsite informații privind acțiunile de prevenție adecvate și punerea în practică, deși în MT și RO legislația reflectă această obligație, urmând îndeaproape formularea din directivă.

3. Concluzii și etapele următoare

Directiva a dus la progrese semnificative în ceea ce privește incriminarea fraudelor și a contrafacerii mijloacelor de plată fără numerar la un nivel comparabil în toate statele membre, ceea ce facilitează cooperarea transfrontalieră a autorităților de aplicare a legii care investighează acest tip de infracțiuni. Statele membre au modificat codurile penale și alte acte legislative relevante, au simplificat procedurile și au creat sau au îmbunătățit sistemele de cooperare. Comisia recunoaște eforturile majore depuse de statele membre pentru transpunerea directivei.

Cu toate acestea, există posibilități încă neexploatate pentru ca directiva să își atingă potențialul maxim dacă statele membre ar pune în aplicare integral toate dispozițiile acesteia. Analiza de până acum sugerează că principalele îmbunătățiri care trebuie realizate de statele membre ar trebui să vizeze articolul 2 litera (d), care conține definiția monedei virtuale; articolul 7 privind infracțiunile legate de instrumentele utilizate pentru săvârșirea infracțiunilor și articolul 8 alineatul (2) privind tentativa; articolul 9 alineatul (6) privind pedepsele aplicabile persoanelor fizice în cazul în care infracțiunea este săvârșită în cadrul unei organizații criminale; articolul 14 privind schimbul de informații; și articolul 16 privind asistența și sprijinul acordat victimelor.

Comisia va continua să ofere sprijin statelor membre în punerea în aplicare a directivei. În special, o cerere de propuneri specifică va fi publicată în 2023.

Comisia se angajează să garanteze că transpunerea este finalizată în întreaga UE și că dispozițiile sunt puse în aplicare în mod corect. Aceasta include monitorizarea conformității măsurilor naționale cu dispozițiile corespunzătoare din directivă. Acolo unde este necesar, Comisia va face uz de competențele de asigurare a respectării legii care îi sunt conferite prin tratate, prin intermediul procedurilor de constatare a neîndeplinirii obligațiilor.