Conselho da
União Europeia

Bruxelas, 11 de julho de 2023
(OR. en)

11761/23

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

NOTA DE ENVIO

de:	Secretária-geral da Comissão Europeia, com a assinatura de Martine DEPREZ, diretora
data de receção:	10 de julho de 2023
para:	Thérèse BLANCHET, secretária-geral do Conselho da União Europeia
n.° doc. Com.:	COM(2023) 363 final
Assunto:	RELATÓRIO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO que avalia em que medida os Estados-Membros adotaram as medidas necessárias para dar cumprimento à Diretiva (UE) 2019/713 relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário e que substitui a Decisão-Quadro 2001/413/JAI do Conselho

Envia-se em anexo, à atenção das delegações, o documento COM(2023) 363 final.

Anexo: COM(2023) 363 final

COMISSÃO
EUROPEIA

Bruxelas, 10.7.2023
COM(2023) 363 final

RELATÓRIO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO

que avalia em que medida os Estados-Membros adotaram as medidas necessárias para dar cumprimento à Diretiva (UE) 2019/713 relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário e que substitui a Decisão-Quadro 2001/413/JAI do Conselho

1. Introdução

A fraude e a contrafação de meios de pagamento que não em numerário, como os cartões de crédito ou de pagamento, são uma fonte de rendimento para a criminalidade organizada e possibilitam outras atividades criminosas, como o terrorismo, o tráfico de droga e o tráfico de seres humanos. Tais crimes causam perdas significativas: o valor total das transações fraudulentas com cartões emitidos no Espaço Único de Pagamentos em Euros (SEPA) ascendeu a 1,87 mil milhões de EUR em 2019[1].A grande maioria das transações fraudulentas está relacionada com fraude sem presença física do cartão: em 2019, 80 % do valor da fraude com cartões resultou de transações sem presença física do cartão, ou seja, pagamentos através da Internet, do correio ou do telefone[2]. A fraude sem presença física do cartão foi responsável por 1,50 mil milhões de EUR de perdas por fraude em 2019, o que representa um aumento de 4,3 % em relação ao ano anterior[3].

Existe uma clara dimensão transfronteiriça: mais de metade do valor total da fraude em 2019 estava relacionado com transações transfronteiriças no SEPA. Do ponto de vista geográfico, as transações nacionais representaram 89 % do valor de todas as transações com cartão em 2019, mas apenas 35 % das transações fraudulentas. As transações transfronteiriças no SEPA representaram 9 % de todas as transações com cartão em termos de valor, mas 51 % das fraudes comunicadas[4].

Para combater eficazmente estes crimes, os Estados-Membros devem definir em comum os atos que devem ser considerados fraude e contrafação de meios de pagamento que não em numerário. Necessitam igualmente de níveis aproximados de sanções e de meios operacionais para comunicar as infrações e proceder à troca de informações entre autoridades. Assim, a 17 de abril de 2019, o Parlamento Europeu e o Conselho adotaram a Diretiva 2019/713 (a seguir designada por «diretiva») relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário e que substitui a Decisão-Quadro 2001/413/JAI do Conselho[5]. O presente relatório dá resposta ao requisito previsto no artigo 21.º da diretiva.

1.1 Objetivos e âmbito de aplicação da diretiva

A diretiva tem como objetivos aproximar o direito penal dos Estados-Membros[6] no domínio da fraude e da contrafação de meios de pagamento que não em numerário e melhorar a cooperação entre as autoridades competentes. Para o efeito, a diretiva estabelece regras mínimas relativas à definição das infrações penais e das sanções. O âmbito de aplicação da diretiva é vasto, abrangendo qualquer «dispositivo, objeto ou registo protegido não corpóreo ou corpóreo, ou uma combinação destes elementos, diferente da moeda em curso legal, e que,

---

1 Banco Central Europeu, Sétimo relatório sobre fraude com cartões, disponível em 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/PT/TXT/?uri=uriserv%3AOJ.L_.2019.123.01.0018.01.POR.

6 Doravante e salvo indicação expressa em contrário, as expressões «Estados-Membros» ou «todos os Estados-Membros» remetem para os Estados-Membros vinculados pela diretiva, ou seja, todos os Estados-Membros da UE, com exceção da Dinamarca e da Irlanda, que não participaram na adoção da diretiva, em conformidade com o Protocolo relativo à posição da Dinamarca, anexo ao Tratado da União Europeia (TUE) e ao Tratado sobre o Funcionamento da União Europeia (TFUE) e em conformidade com o Protocolo n.º 21 relativo à posição do Reino Unido e da Irlanda, respetivamente.

por si só ou em conjugação com um procedimento ou um conjunto de procedimentos, permite ao titular ou utilizador transferir dinheiro ou valor monetário, inclusive através de meios de troca digitais» [artigo 2.º, alínea a)[7]]. Por exemplo, uma aplicação móvel de pagamento em conjunto com o procedimento de autorização (como o PIN) seria abrangida por esta definição. As moedas virtuais também são abrangidas pelo âmbito de aplicação da diretiva [artigo 2.º, alínea d), e artigo 6.º].

A diretiva define infrações penais específicas, nomeadamente:

- utilização fraudulenta de instrumentos de pagamento que não em numerário (artigo 3.º),
- infrações relacionadas com a utilização fraudulenta de instrumentos de pagamento corpóreos que não em numerário (artigo 4.º),
- infrações relacionadas com a utilização fraudulenta de instrumentos de pagamento não corpóreos que não em numerário (artigo 5.º),
- fraude relacionada com sistemas de informação (artigo 6.º),
- disponibilização ilegal de instrumentos utilizados para cometer as infrações mencionadas (artigo 7.º).

Acresce que a diretiva alarga **a responsabilidade penal** à instigação e à cumplicidade das pessoas singulares e/ou coletivas na prática e na tentativa da prática de uma das infrações anteriormente mencionadas (artigo 8.º).

No artigo 9.º estão previstos níveis mínimos de **sanções** máximas aplicáveis às infrações enunciadas na diretiva.

Os artigos seguintes estabelecem condições mínimas de **responsabilidade das pessoas coletivas** (artigo 10.º) e sanções, que devem incluir multas ou coimas, e fornecem uma lista indicativa das outras sanções que podem ser-lhes aplicadas (artigo 11.º).

O objetivo do artigo 12.º é garantir que os autores de infrações, tal como definidos na diretiva, sejam objeto de uma ação penal relativamente às infrações previstas nos artigos 3.º a 8.º da diretiva. A **competência jurisdicional** de um Estado-Membro deve ser estabelecida se a) a infração for cometida, no todo ou em parte, no seu território, e/ou b) o autor da infração for um dos seus nacionais. Por outras palavras, o artigo 12.º, n.º 1, alínea a), da diretiva estabelece o princípio da territorialidade, enquanto a alínea b) aplica o princípio da nacionalidade ativa.

O artigo 13.º, n.º 1, da diretiva estabelece que **os instrumentos de investigação** utilizados para investigar e promover a ação penal no que respeita às infrações previstas nos artigos 3.º a 8.º devem ser eficazes, proporcionais ao crime cometido e disponibilizados às pessoas, às unidades ou aos serviços responsáveis. As informações relativas às infrações previstas nos artigos 3.º a 8.º devem chegar sem atrasos indevidos às autoridades responsáveis por investigar ou promover a ação penal no que respeita àquelas infrações, nos termos do artigo 13.º, n.º 2, da diretiva.

No que se refere ao intercâmbio de informações, o artigo 14.º estabelece que os Estados-Membros devem assegurar a existência de **pontos de contacto** operacionais nacionais

[7] Todos os artigos mencionados referem-se aos artigos da diretiva, salvo indicação em contrário.

disponíveis 24 horas por dia e sete dias por semana, de modo que possam dar resposta aos pedidos de assistência urgentes no prazo máximo de oito horas.

Além disso, o artigo 15.º, n.º 1, da diretiva exige que os Estados-Membros criem canais adequados para **facilitar a comunicação das infrações** referidas nos artigos 3.º a 8.º às autoridades públicas, sem atrasos indevidos. Em especial, as instituições financeiras são convidadas a comunicar as suspeitas de fraude às autoridades responsáveis pela aplicação da lei e às autoridades judiciais (artigo 15.º, n.º 2). A comunicação de tais infrações é muitas vezes o ponto de partida da investigação penal (considerando 27).

Por último, os artigos 16.º e 17.º da diretiva tratam da **assistência e apoio às vítimas** e da **prevenção**, respetivamente.

1.2 Objetivo e metodologia do relatório

O artigo 20.º da diretiva exige que os Estados-Membros ponham em vigor as disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento à mesma até 31 de maio de 2021 e que comuniquem à Comissão esse facto.

O presente relatório dá resposta ao requisito constante do artigo 21.º da diretiva, segundo o qual a Comissão deve apresentar ao Parlamento Europeu e ao Conselho um relatório destinado a avaliar em que medida os Estados-Membros tomaram as medidas necessárias para dar cumprimento à mesma. O relatório – o primeiro ao abrigo do artigo 21.º – apresenta uma panorâmica das principais medidas de transposição adotadas pelos Estados-Membros.

A transposição por parte dos Estados-Membros envolveu a recolha de informações sobre as medidas legislativas e administrativas relevantes, a análise dessas informações, a elaboração de nova legislação ou, na maior parte dos casos, a alteração de atos existentes, o acompanhamento de todo o processo até à adoção e, por último, a comunicação à Comissão.

Até à data da transposição (31 de maio de 2021), nove Estados-Membros tinham comunicado à Comissão a conclusão da transposição da diretiva e notificado as respetivas medidas de transposição. Em julho de 2021, a Comissão instaurou processos por infração contra os restantes 16 Estados-Membros por não comunicação das medidas nacionais de transposição: AT, BE, BG, CY, CZ, EL, ES, HR, IT, LU, LV, MT, PL, PT, RO e SI[8]. Embora 15 Estados-Membros tenham entretanto notificado as suas medidas de transposição, em 30 de abril de 2023 ainda se encontrava pendente um processo de infração por não comunicação das medidas nacionais de transposição contra a BG[9].

A descrição e a análise contidas no presente relatório baseiam-se nas informações relativas às medidas nacionais de transposição que os Estados-Membros comunicaram até 31 de janeiro de 2023. As notificações recebidas após essa data não foram tomadas em consideração. Todas as medidas notificadas referentes às legislações nacionais foram tomadas em consideração, bem como as decisões judiciais e, sempre que adequado, a doutrina comum. Além disso, no decurso da análise, a Comissão contactou diretamente os Estados-Membros, sempre que

[8] No presente documento, os Estados-Membros são designados de forma abreviada, em conformidade com: https://publications.europa.eu/code/pt/pt-5000600.htm.

[9] As decisões da Comissão relativas a processos por infração podem ser consultadas em: http://ec.europa.eu/atwork/applying-eu-law/infringements-proceedings/infringement_decisions/?lang_code=en.

necessário, para obter informações ou esclarecimentos adicionais. Todas as informações recolhidas foram tomadas em consideração para efeitos da análise.

Além das questões identificadas no presente relatório, poderão existir outros obstáculos à transposição, outras disposições não comunicadas à Comissão ou futuros desenvolvimentos legislativos e não legislativos. Por conseguinte, o presente relatório não impede a Comissão de prosseguir a avaliação de algumas disposições e de continuar a apoiar os Estados-Membros na transposição e aplicação da diretiva.

2. Medidas de transposição

2.1 Definições jurídicas

O artigo 2.º estabelece as definições dos principais termos utilizados na diretiva, nomeadamente: instrumento de pagamento que não em numerário; dispositivo, objeto ou registo protegido; meio de troca digital; moeda virtual; sistema de informação; dados informáticos; pessoa coletiva.

Em geral, os Estados-Membros transpuseram as definições com base em disposições legislativas anteriores à diretiva ou adotadas após a sua entrada em vigor. Em alguns casos, embora não existam disposições que estabeleçam especificamente definições, as infrações são transpostas através de disposições gerais do código penal que têm um âmbito de aplicação mais vasto como, por exemplo, disposições relativas ao furto. Por conseguinte, a não comunicação de uma transposição literal da definição não indica necessariamente que a definição não está completa ou que não é conforme.

Além disso, várias definições fazem referência cruzada a definições estabelecidas noutras diretivas.

a) Instrumentos de pagamento que não em numerário

A avaliação revelou pelo menos um caso de transposição incompleta, uma vez que a definição estabelecida pela Decisão-Quadro 2001/413/JAI do Conselho não tinha sido atualizada. Por conseguinte, nesse caso, a definição refere-se apenas a instrumentos de pagamento corpóreos e não abrange «um dispositivo, objeto ou registo protegido [...], ou uma combinação destes elementos», como previsto na definição da diretiva.

b) Dispositivo, objeto ou registo protegido

Vários Estados-Membros não transpuseram esta definição (BG, CZ, EE, ES, FI, HR, LT, NL, PL, PT, RO e SI). Tal não é necessariamente considerado um caso de incumprimento, uma vez que, geralmente, o significado é autoexplicativo ou pode ser deduzido da redação da definição de instrumento de pagamento que não em numerário. Em alguns países, o conceito é explicado nos trabalhos preparatórios.

c) Meios de pagamento digitais e moeda virtual

Ambas as definições são essenciais para a Diretiva 2019/713, cujo principal objetivo é remediar o facto de a Decisão-Quadro 2001/413/JAI já não refletir a realidade atual e fazer face de forma insuficiente aos novos desafios e desenvolvimentos tecnológicos, como as moedas virtuais e os pagamentos móveis, que era necessário incluir para garantir uma resposta abrangente ao fenómeno e colmatar lacunas involuntárias a nível da criminalização.

A principal dificuldade que se coloca na transposição é o âmbito de aplicação da moeda virtual, definida no artigo 2.º, alínea d), da diretiva. Embora o termo «moeda eletrónica» se encontre definido em todos os Estados-Membros, frequentemente em resultado da transposição da Diretiva Moeda Eletrónica[10], a definição e o âmbito de aplicação do termo «moeda virtual» nem sempre são claros.

[10] Diretiva 2009/110/CE do Parlamento Europeu e do Conselho, de 16 de setembro de 2009, relativa ao acesso à atividade das instituições de moeda eletrónica, ao seu exercício e à sua supervisão prudencial, que altera as Diretivas 2005/60/CE e 2006/48/CE e revoga a Diretiva 2000/46/CE (JO L 267 de 10.10.2009).

Na HU, a moeda virtual é considerada como um bem e um dado eletrónico, podendo ser objeto de perda de bens e de apreensão. Do mesmo modo, na Polónia, a moeda virtual não está definida na legislação e existe um certo grau de incerteza quanto ao facto de ser abrangida pelas diferentes infrações pertinentes para a transposição da diretiva, embora alguns autores considerem que a moeda virtual poderia ser abrangida pelas disposições do Código Penal que regulam as infrações relativas à informação, ao suporte de dados ou aos dados de informação.

Muitos Estados-Membros transpuseram estas definições mediante regras financeiras e não no direito penal (AT, BE, BG, CY, CZ, DE, EE, EL, ES, HR, HU, LT, LU, LV e SI). No entanto, nalguns destes casos existe uma referência cruzada às disposições relevantes da legislação nacional que estabelece as infrações. Por último, em três Estados-Membros (IT, MT e RO), ambas as definições são transpostas para o Código Penal.

d) Sistema de informação

O artigo 2.º, alínea e), define «sistema de informação» por referência cruzada ao artigo 2.º, alínea a), da Diretiva 2013/40/UE. Todos os Estados-Membros transpuseram a definição em conformidade com a diretiva.

e) Dados informáticos

Os dados informáticos são definidos no artigo 2.º, alínea f), por referência cruzada ao artigo 2.º, alínea b), da Diretiva 2013/40/UE. Todos os Estados-Membros transpuseram o artigo 2.º, alínea f), em conformidade com a diretiva.

f) Pessoa coletiva

Por último, o artigo 2.º, alínea g), define «pessoa coletiva». Quase todos os Estados-Membros transpuseram este termo para a sua legislação. A única exceção é a SE, que não define «pessoa coletiva». O termo mais próximo utilizado na transposição é «empresa». Este termo não é definido em nenhum texto jurídico, nem na doutrina nem na jurisprudência.

2.2 Infrações penais específicas

a) Utilização fraudulenta de instrumentos de pagamento que não em numerário

O artigo 3.º, alínea a), da diretiva exige que os Estados-Membros tomem as medidas necessárias para assegurar que a utilização fraudulenta de um instrumento de pagamento que não em numerário furtado ou roubado, apropriado ou obtido de outra forma ilícita, quando cometida com dolo, seja punível como infração penal.

Vinte e cinco Estados-Membros transpuseram o artigo 3.º, alínea a), da diretiva. Dos 25 países, 14 transpuseram a diretiva através de uma disposição específica sobre a utilização fraudulenta de instrumentos de pagamento que não em numerário (AT, CY, ES, FI, HU, IT, LT, MT, NL, PT, RO, SE, SI e SK). Os restantes Estados-Membros referiram-se a infrações mais gerais, como a fraude e a contrafação recorrendo a meios informáticos, ou a fraude relacionada com meios de pagamento, não se limitando aos instrumentos de pagamento que não em numerário (BE, BG, CZ, DE, EE, EL, FR, HR, LU, LV, PL, SE e SK).

A legislação da HR não se refere à utilização de instrumentos de pagamento furtados ou roubados, apropriados ou obtidos de outra forma ilícita; a disposição de transposição da HU refere-se apenas a instrumentos de pagamento eletrónicos que não em numerário.

Nos termos do artigo 3.º, alínea b), da diretiva, os Estados-Membros devem tomar as medidas necessárias para assegurar que a utilização fraudulenta de um instrumento de pagamento que não em numerário contrafeito ou falsificado, quando cometida com dolo, seja punível como infração penal.

O artigo 3.º, alínea b) foi, de um modo geral, inteiramente transposto.

Para transpor a diretiva, 15 Estados-Membros remetem para disposições nacionais relativas a instrumentos de pagamento que não em numerário (AT, CY, DE, EE, ES, FI, HR, HU, IT, LT, MT, NL, PT, RO e SI), enquanto a legislação nacional de transposição em dez Estados-Membros abrange infrações mais gerais, como o furto ou a fraude, ou infrações relacionadas com instrumentos de pagamento, mas não especificamente instrumentos que não em numerário (BE, BG, CZ, EL, FR, LU, LV, PL, SE e SK).

b) Infrações relacionadas com a utilização fraudulenta de instrumentos de pagamento corpóreos que não em numerário

O artigo 4.º da diretiva exige que os Estados-Membros tomem as medidas necessárias para garantir que os atos intencionais enumerados nas suas alíneas sejam puníveis como infrações penais. As alíneas incluem o furto ou outra forma de apropriação ilícita de um instrumento de pagamento corpóreo que não em numerário [alínea a)]; a contrafação ou falsificação fraudulentas de um instrumento de pagamento corpóreo que não em numerário [alínea b)]; a posse de um instrumento de pagamento corpóreo que não em numerário furtado, roubado ou apropriado de outra forma ilícita, ou que tenha sido objeto de contrafação ou de falsificação, para utilização fraudulenta [alínea c)]; a aquisição para si próprio ou para terceiro, incluindo a receção, a apropriação, a compra, a transferência, a importação, a exportação, a venda, o transporte ou a distribuição de um instrumento de pagamento corpóreo que não em numerário furtado, roubado, contrafeito ou falsificado, para utilização fraudulenta [alínea d)].

Embora o artigo 4.º pareça ter sido transposto, na sua maior parte, de forma mais ou menos literal, em alguns casos a transposição nacional levanta questões no que se refere aos atos específicos de aquisição, para si próprio ou para terceiro, de um instrumento de pagamento corpóreo que não em numerário furtado, roubado, contrafeito ou falsificado, para utilização fraudulenta.

c) Infrações relacionadas com a utilização fraudulenta de instrumentos de pagamento não corpóreos que não em numerário

O artigo 5.º da diretiva criminaliza as condutas relacionadas com a utilização fraudulenta de instrumentos de pagamento não corpóreos que não em numerário. A análise concluiu que este artigo não parece ter levantado dificuldades de transposição. Na maioria dos casos, a disposição nacional aplica-se aos instrumentos de pagamento corpóreos e não corpóreos que não em numerário. Cerca de metade dos Estados-Membros transpuseram o artigo 5.º da diretiva através de disposições de caráter mais geral (BE, BG, DE, EE, FI, HR, FR, LV, PL, SE e SK) e mais de metade transpuseram-no através de uma disposição especificamente relacionada com a utilização fraudulenta de instrumentos de pagamento que não em numerário (AT, CY, CZ, EL, ES, HU, IT, LT, LU, NL, PT, RO e SI).

d) Fraude relacionada com sistemas de informação

O artigo 6.º da diretiva obriga os Estados-Membros a garantir que os atos de transferir ou fazer transferir dinheiro, valor monetário ou moedas virtuais que causem desse modo um prejuízo patrimonial ilícito para outrem, a fim de obter benefícios ilícitos para si próprio ou para terceiro sejam puníveis como infrações penais, quando praticados com dolo através de obstrução ou interferência no funcionamento de um sistema de informação, sem direito a tal [artigo 6.º, alínea a)]; ou introdução, alteração, eliminação, transmissão ou supressão de dados informáticos, sem direito a tal [artigo 6.º, alínea b)]. Todos os Estados-Membros transpuseram o artigo 6.º.

e) Instrumentos utilizados para cometer infrações

O artigo 7.º da diretiva exige que os Estados-Membros tomem as medidas necessárias para assegurar que sejam puníveis como infrações penais a produção, a aquisição para si próprio ou para terceiro, ou a disponibilização de um dispositivo ou instrumento, de dados informáticos ou de quaisquer outros meios principalmente concebidos ou especificamente adaptados para cometer uma das infrações previstas no artigo 4.º, alíneas a) e b), no artigo 5.º, alíneas a) e b), ou no artigo 6.º, pelo menos quando esses atos forem praticados com a intenção de que esses meios sejam utilizados.

A grande maioria dos Estados-Membros transpôs o artigo 7.º da diretiva (AT, CY, CZ, DE, EE, ES, FI, FR, HR, IT, LT, LV, NL, RO, SE, SI e SK).

Seis países transpuseram o artigo 7.º da diretiva através de disposições que remetem para disposições mais amplas, quer sobre infrações gerais, como o furto, quer sobre instrumentos financeiros e meios de pagamento (BG, FI, FR, LV, SE e SK). Dezassete países transpuseram-no através de uma disposição específica relacionada com os instrumentos utilizados para cometer as diferentes infrações da diretiva relacionadas com instrumentos de pagamento corpóreos ou não corpóreos que não em numerário (AT, CY, CZ, DE, EE, EL, ES, HR, HU, IT, LT, LU, MT, NL, PL, RO e SI).

Cinco Estados-Membros parecem ter enfrentado dificuldades na transposição (BE, BG, HU, PL e PT).

2.3 Regras gerais para as infrações em causa

a) Instigação, cumplicidade tentativa

Nos termos do artigo 8.º, n.º 1, da diretiva, os Estados-Membros devem assegurar que a instigação e a cumplicidade na comissão de uma infração referida nos artigos 3.º a 7.º sejam puníveis como infrações penais.

Todos os Estados-Membros transpuseram esta disposição. A grande maioria dos Estados-Membros transpôs a diretiva através de um artigo pré-existente sobre incitamento e cumplicidade em geral (AT, BE, BG, CZ, DE, EE, EL, ES, FI, FR, HR, HU, IT, LT, LU, LV, NL, PL, PT, RO, SE, SI e SK). No entanto, dois Estados-Membros decidiram adotar uma nova disposição, que se aplica apenas no contexto das infrações previstas na diretiva (CY, MT).

A primeira frase do artigo 8.º, n.º 2, da diretiva exige que os Estados-Membros assegurem que a tentativa de comissão de uma das infrações previstas no artigo 3.º, no artigo 4.º, alíneas a), b) ou d), no artigo 5.º, alíneas a) ou b), ou no artigo 6.º seja punível como infração penal. Todos os Estados-Membros parecem ter transposto inteiramente esta disposição, exceto BE, LU e SI.

Também neste caso, a maioria dos Estados-Membros transpôs a diretiva através de uma disposição já existente aplicável à tentativa em geral (AT, BG, CZ, EE, EL, ES, FR, HR, HU, IT, LT, LV, NL, PL, PT, SE e SK). Os demais incluíram-na numa medida especial de transposição (CY, DE, FI, MT e RO).

Os Estados-Membros devem igualmente assegurar que pelo menos a tentativa de aquisição fraudulenta, para si próprio ou para terceiro de um instrumento de pagamento não corpóreo que não em numerário obtido de forma ilícita, contrafeito ou falsificado, seja punível como infração penal [artigo 5.º, alínea d), e artigo 8.º, n.º 2, segunda frase].

A avaliação revelou que a criminalização da tentativa pode estar sujeita a limitações não previstas na diretiva em dois Estados-Membros (HR e SI).

Todos os restantes Estados-Membros transpuseram as disposições pertinentes da diretiva. Fizeram-no quer através de um artigo sobre a tentativa em geral (AT, BE, BG, CZ, IT, EE, EL, ES, FR, HU, LT, LU, LV, NL, PL, PT, SE e SK), quer através de uma medida especial de transposição (CY, DE, FI, MT e RO).

b) Sanções

O artigo 9.º estabelece que as infrações previstas nos artigos 3.º a 8.º devem ser puníveis com sanções penais efetivas, proporcionadas e dissuasivas e prevê a pena de prisão máxima para as diferentes infrações.

Embora, de um modo geral, os Estados-Membros tenham transposto o artigo 9.º da diretiva, a avaliação identificou possíveis problemas relacionados com o âmbito da definição no que se refere ao artigo 9.º, n.º 2, na HR e ao artigo 9.º, n.º 6, na BE, CZ, HR e HU.

A comparação das sanções estabelecidas pelos Estados-Membros para as diferentes infrações é complicada porque as infrações são abrangidas tanto por disposições gerais como por disposições específicas. Ao transporem a diretiva através de disposições relativas a infrações gerais, os Estados-Membros basearam-se em várias disposições nacionais para criminalizar um dos atos proibidos pela diretiva. Tal conduz a várias sanções penais máximas aplicáveis a esta infração específica e implica que a sanção máxima efetiva dependa de cada caso específico, da abordagem seguida pelos tribunais e das regras nacionais em matéria de cúmulo de sanções. A título de exemplo, na PL, a regra é que um ato só pode constituir uma infração. No caso de um comportamento apresentar características de duas ou mais disposições de direito penal, o tribunal deve escolher uma só infração. Pelo contrário, na BG, nos casos em que a parte especial do Código Penal preveja a aplicação de duas ou mais sanções penais concomitantemente para um determinado crime, o tribunal deve determinar a medida de cada sanção penal de modo que a sua soma cumpra os objetivos gerais da sanção penal.

Além disso, as disposições podem prever circunstâncias agravantes suscetíveis de aumentar o limite máximo e conduzir a um aumento das sanções. A sanção penal máxima depende, portanto, da forma como a infração é cometida. Por exemplo, na HR, a disposição geral relativa à apropriação ilegítima prevê uma sanção penal máxima de cinco anos de prisão. No entanto, se o autor da infração usar a força, a sanção penal máxima é de 10 anos e, se a ação

resultar em ganhos materiais substanciais, o infrator pode ser condenado a 12 anos de prisão. Na DE, a falsificação de instrumentos de pagamento corpóreos que não em numerário é punida com uma pena máxima de cinco anos de prisão. No entanto, se o autor da infração tiver agido com fins comerciais, a sanção penal será de 10 anos, no máximo.

A avaliação revelou igualmente que, na maioria dos casos, os limiares previstos na legislação nacional são mais severos do que os estabelecidos pela diretiva. A diferença pode ser significativa: a contrafação de moeda é punível com uma sanção penal máxima de 15 anos na BG e no LU e com uma sanção penal máxima de 25 anos na PL. Apenas dois Estados-Membros preveem sanções penais máximas idênticas (ou muito próximas) às previstas na diretiva (AT e MT).

c) Responsabilidade das pessoas coletivas

A avaliação revelou que 16 Estados-Membros transpuseram o artigo 10.º da diretiva através de uma disposição geral já existente no seu Código Penal (AT, CZ, BE, BG, DE, EE, ES, FR, HR, HU, LU, LV, NL, PT, RO e SE), enquanto nove Estados-Membros o transpuseram através de uma lei específica relativa à responsabilidade das pessoas coletivas no contexto da diretiva (CY, EL, FI, IT, LT, MT, PL, SI e SK).

d) Sanções aplicáveis a pessoas coletivas

O artigo 11.º da diretiva exige que os Estados-Membros estabeleçam sanções eficazes, proporcionadas e dissuasivas, sob a forma de multas ou coimas, também para as pessoas coletivas. Todos os Estados-Membros estabeleceram sanções deste tipo.

O artigo 11.º prevê a possibilidade de os Estados-Membros incluírem várias sanções específicas aplicáveis a pessoas coletivas, tais como a exclusão do direito a benefícios públicos ou a liquidação judicial. Seis Estados-Membros não recorreram de todo à possibilidade prevista no artigo 11.º da diretiva (AT, BG, EE, FI, NL e SE). Os restantes 19 países transpuseram a totalidade ou parte do artigo 11.º (BE, CY, CZ, DE, EL, ES, FR, HR, HU, IT, LT, LU, LV, MT, PL, PT, RO, SI e SK).

e) Competência jurisdicional

Este artigo, que obriga os Estados-Membros a determinar a sua competência relativamente às infrações cometidas no seu território ou por um dos seus nacionais, é transposto para as disposições gerais do Código Penal ou do Código de Processo Penal de todos os Estados-Membros. Por conseguinte, o princípio da territorialidade e o princípio da nacionalidade ativa são de aplicação geral e não são específicos das infrações reguladas pela diretiva. Além disso, o artigo 12.º foi também transposto por CY para a lei nacional relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário e por PT para a lei relativa à cibercriminalidade.

Todos os Estados-Membros transpuseram o artigo 12.º, n.º 1, alíneas a) e b).

O artigo 12.º, n.º 3, permite aos Estados-Membros determinar a sua competência relativamente às infrações previstas nos artigos 3.º a 8.º da diretiva cometidas fora do seu território, quando, nomeadamente: a) a infração seja cometida por alguém que tenha a sua residência habitual no seu território; b) a infração seja cometida em benefício de uma pessoa coletiva estabelecida no seu território; ou c) a infração seja cometida contra um dos seus nacionais ou contra uma pessoa que resida habitualmente no seu território. Catorze Estados-Membros (BE, CY, CZ, DE, EL, ES, FI, HR, LT, LV, MT, NL, SE e SK) recorreram à

possibilidade prevista no artigo 12.º, n.º 3, alínea a); 12 Estados-Membros (BE, CY, CZ, EL, FI, LV, MT, NL, PL, PT, SI e SK) transpuseram o artigo 12.º, n.º 3, alínea b); e 16 Estados-Membros (AT, BG, CY, CZ, DE, EE, EL, FI, FR, HR, HU, LV, MT, RO, SE e SI) alargaram a sua competência em conformidade com o artigo 12.º, n.º 3, alínea c). No que diz respeito a esta alínea c), na BG, DE, EE, HU, RO e SI foi estabelecida a competência sobre uma infração cometida fora do seu território quando a infração seja cometida (apenas) contra um dos seus nacionais, omitindo assim as pessoas que residem habitualmente no seu território. A AT prevê que as infrações cometidas no estrangeiro sejam objeto de uma ação penal no sistema de justiça penal austríaco se o autor da infração e a vítima forem austríacos. CY, CZ, EL, FI, LV e MT utilizaram as três disposições facultativas previstas no artigo 12.º, n.º 3.

2.4 Questões operacionais

a) Investigações e cooperação eficazes

Em todos os Estados-Membros, os instrumentos de investigação para a investigação e repressão das infrações referidas nos artigos 3.º a 8.º não estão explicitamente incluídos na legislação de transposição da diretiva, mas sim em legislação mais geral, como os códigos de processo penal. Normalmente, a possibilidade de utilizar um instrumento de investigação num determinado caso está relacionada com a sanção aplicada à infração em questão; assim, tal como já referido na disposição da diretiva, os instrumentos de investigação utilizados na luta contra a criminalidade organizada ou noutros casos de criminalidade grave estarão igualmente disponíveis para investigar e reprimir as infrações previstas na diretiva. O caráter excecional de alguns instrumentos de investigação e a necessidade de proporcionalidade com a infração estão, na maior parte dos casos, previstos nas disposições jurídicas pertinentes e/ou na Constituição.

As informações relativas às infrações previstas nos artigos 3.º a 8.º devem chegar sem atrasos indevidos às autoridades responsáveis por investigar ou promover a ação penal no que respeita àquelas infrações, , nos termos do artigo 13.º, n.º 2, da diretiva. Por outras palavras, as autoridades responsáveis pela aplicação da lei e outras autoridades competentes devem poder aceder atempadamente a informações pertinentes por forma a investigarem e a promoverem a ação penal no que respeita às infrações referidas na diretiva (considerando 22). O Código de Processo Penal prevê frequentemente vários sistemas de denúncia para que as infrações penais (na aceção dos artigos 3.º a 8.º da diretiva) possam ser denunciadas de forma eficaz e rápida. Estes sistemas de informação incluem: um dever de denunciar dos organismos e autoridades públicas; um sistema de denúncia de irregularidades; um procedimento de queixa; a obrigação de os prestadores de serviços de pagamento comunicarem os incidentes operacionais ou de segurança graves; e o direito de os particulares comunicarem os incidentes. Além disso, algumas leis mais específicas podem garantir que as notificações de incidentes de segurança (incluindo as notificações de atos criminosos graves, como a aquisição não autorizada, a falsificação e a alteração de um meio de pagamento) sejam comunicadas às autoridades competentes o mais rapidamente possível. Tais leis foram comunicadas por AT, CZ, LT, FI, MT e PT.

A condição segundo a qual as informações apresentadas devem «chegar às autoridades competentes sem atrasos indevidos» não é, na maioria das vezes, transposta de forma explícita.

b) Intercâmbio de informações

O intercâmbio de informações entre as autoridades nacionais responsáveis pela aplicação da lei para efeitos de investigação e repressão de crimes, incluindo os referidos nos artigos 3.º a 8.º da diretiva, pode ser facilitado através de pontos de contacto operacionais (considerando 26). A primeira frase do artigo 14.º, n.º 1, da diretiva garante que os Estados-Membros estabelecem efetivamente esses pontos de contacto e que estes estão disponíveis 24 horas por dia, sete dias por semana. Além disso, a segunda frase obriga os Estados-Membros a disporem de procedimentos que permitam dar uma resposta pronta aos pedidos de assistência urgentes e que permitam à autoridade competente responder no prazo máximo de oito horas a contar da receção do pedido, indicando pelo menos se o pedido será atendido, sob que forma será dada a resposta e qual o prazo estimado de resposta.

Os seguintes Estados-Membros decidiram utilizar um ponto de contacto operacional existente para os fins descritos na diretiva: AT, BE, CY, EE, EL, ES, FR, HU, IT, LT, LV, NL, PL, PT e SE.

O quadro 1 apresenta uma panorâmica dos pontos de contacto existentes. Não foram identificados pontos de contacto na BG, CZ, LU, SI e HR.

Quadro 1 Pontos de contacto operacionais

EM	Ponto de contacto	EM	Ponto de contacto
AT	Serviço Federal de Polícia Judiciária	**EE**	Ministério da Justiça
BE	Direção de Informação Policial Operacional	**FI**	Serviço Nacional de Informação
BG	N/A	**FR**	Divisão de relações internacionais da Direção Central da Polícia Judiciária
CY	Polícia Cipriota	**HR**	N/A
CZ	N/A	**HU**	Centro de Cooperação Penal Internacional (NEBEK)
DE	16 gabinetes federados da polícia judiciária e um gabinete federal da polícia judiciária – pontos de contacto centrais para a cibercriminalidade	**MT**	Polícia Maltesa
EL	Polícia Helénica (Divisão de Cooperação Policial Internacional)	**ES**	Célula de Coordenação de Emergência
IT	Departamento de Operações Internacionais do Serviço de Cooperação Policial Internacional	**NL**	Centro Nacional de Assistência Jurídica Internacional (LIRC)
LT	2.ª Divisão do Conselho de Gestão da Força do Departamento de Polícia do Ministério do Interior da República da Lituânia e do Conselho de Relações Internacionais do Serviço de Polícia Judiciária da Lituânia	**PL**	Direção-Geral da Polícia
LV	Polícia Nacional	**PT**	Polícia Judiciária
RO	Secção de Instrução e Investigação Criminal da Procuradoria-Geral da República	**SE**	Autoridade Policial
SI	N/A	**SK**	Departamento de Polícia Judiciária do *Presidium* das Forças Policiais da República Eslovaca

O artigo 14.º, n.º 1, segunda frase, da diretiva foi aplicado na prática em alguns Estados-Membros. Não foi possível encontrar informações sobre os procedimentos aplicáveis aos pedidos urgentes na BE, BG, CZ, LV, RO, FR, HR, LU, NL, PL, SE e SK.

c) Comunicação de infrações penais

Os Estados-Membros são igualmente obrigados a disponibilizar canais de comunicação adequados. Tais canais para comunicar suspeitas de fraude ou, de um modo mais geral, eventuais infrações penais podem ser previstos em atos legislativos. Frequentemente, os Estados-Membros estabeleceram a obrigação de denunciar um crime para determinadas categorias de pessoas (singulares e coletivas) (em grande medida em conformidade com o artigo 15.º, n.º 2), enquanto as vítimas e outros «observadores» têm a possibilidade (mas não a obrigação) de denunciar. Tais disposições legais são geralmente complementadas por uma aplicação prática.

Em todos os Estados-Membros podem ser feitas denúncias escritas ou orais à polícia e/ou às autoridades judiciais. Além disso, alguns Estados-Membros criaram canais de comunicação adicionais:

A legislação federal da AT prevê vários sistemas de comunicação para que as infrações penais na aceção dos artigos 3.º a 8.º da diretiva possam ser notificadas de forma eficaz e rápida: 1) o dever de denunciar dos organismos e autoridades públicas; 2) o sistema de denúncia do gabinete do Ministério Público encarregado dos Assuntos Económicos e da Corrupção; 3) o sistema de denúncia de irregularidades da Autoridade dos Mercados Financeiros; e 4) a obrigação de os prestadores de serviços de pagamento comunicarem incidentes operacionais ou de segurança graves. Foi criado um gabinete de denúncia específico para a cibercriminalidade no Serviço Federal da Polícia Judiciária. Além disso, o Ministério Federal do Interior está a cooperar com a Câmara Económica Federal. Consequentemente, estão a ser realizadas várias campanhas e enviadas de mensagens para motivar e encorajar o público a denunciar violações relevantes da lei.

Na BE, o Ministério da Economia gere um ponto de contacto único para as vítimas de fraude, burla e engano. Além disso, foi legalmente criado e disponibilizado pela Autoridade dos Serviços e Mercados Financeiros um canal de denúncia para todas as queixas relacionadas com produtos e serviços de crédito ou investimento.

Em CY, a Polícia Cipriota, juntamente com o Banco Central de Chipre e a autoridade nacional encarregada da segurança das redes e dos sistemas de informação, são formalmente designados, através de uma medida legislativa, como as autoridades nacionais competentes responsáveis pelo estabelecimento de canais adequados de denúncia e de comunicação.

O direito penal na CZ obriga as autoridades públicas a denunciar as infrações.

Na DE, as entidades obrigadas são obrigadas a comunicar, sem demora injustificada, as transações suspeitas. Além disso, foram adotadas medidas não legislativas a nível federal, tais como uma parceria público-privada institucionalizada para efeitos de deteção, prevenção, investigação ou repressão das infrações referidas nos artigos 3.º a 8.º da diretiva, bem como uma plataforma para o intercâmbio de informações.

Na EL, para além dos canais gerais de comunicação, o Governo grego criou um serviço público em linha onde os cidadãos podem apresentar diretamente queixas por infrações penais cometidas em linha. Para além disso, as instituições de crédito e outros prestadores de serviços de pagamento são obrigados a comunicar imediatamente ao Banco da Grécia (que tem competência neste tipo de queixas) qualquer caso de fraude.

Em ES, para além dos canais gerais de comunicação de infrações, o Banco de Espanha disponibiliza um canal de comunicação em colaboração com o Instituto Nacional de Cibersegurança.

A legislação italiana garante celeridade na comunicação ao Ministério Público pela polícia judiciária das informações relativas a infrações, obtidas por sua própria iniciativa ou na sequência de uma queixa ou de uma ação judicial. A partilha de informações é também incentivada através de plataformas digitais.

A LT dispõe de múltiplos canais de comunicação para denunciar as infrações referidas nos artigos 3.º a 8.º da diretiva, através de uma página Web (Portal e-Police), através do número de telefone geral de emergência 112, presencialmente, por correio eletrónico, por mensagem de texto e através da aplicação móvel e-Police, bem como por outros meios automáticos. Os prestadores de serviços de pagamento, as instituições financeiras e outras entidades obrigadas, o Banco da Lituânia e o Serviço de Investigação de Crimes Financeiros estão obrigados a notificar às autoridades competentes as suspeitas razoáveis de atos criminosos e/ou outros atos ilícitos.

No LU, está disponível um sítio Web que explica como denunciar as fraudes. A Comissão de Controlo do Setor Financeiro definiu orientações para detetar fraudes financeiras, mas também exige a todos os estabelecimentos sob o seu controlo que comuniquem o mais rapidamente possível quaisquer fraudes e incidentes relacionados com ataques informáticos externos.

Na RO, os funcionários públicos e as pessoas que ocupam cargos de gestão nas autoridades públicas, as pessoas que prestam serviços de interesse público e as pessoas que trabalham em organismos de controlo e supervisão estão obrigadas a denunciar as infrações.

Na SI, todas as autoridades públicas e organizações com autoridade pública têm o dever de denunciar as infrações penais.

Na FR, a plataforma Perceval, criada por um ato jurídico, permite que as vítimas denunciem casos de fraude envolvendo cartões bancários e de contrafação. Existe uma plataforma semelhante para denunciar atos de cibercriminalidade. Além disso, são aplicadas sanções a qualquer pessoa (singular ou coletiva) que não impeça, através da sua ação imediata, um crime, o que pressupõe uma obrigação geral de denúncia.

Na HU, a obrigação de denunciar uma infração penal só está prevista para os membros da autoridade, os funcionários públicos e os organismos profissionais estatutários. O Banco Nacional Húngaro incentiva, no seu sítio Web, as instituições financeiras a comunicarem, sob a forma de parecer, as suspeitas de fraude.

Em MT, o ponto de contacto nacional incentiva a comunicação, em especial pelas instituições financeiras, de suspeitas de fraude e contrafação de meios de pagamento que não em numerário.

Em PT, para além do canal de denúncia legalmente estabelecido, está disponível um Sistema de Denúncia de Cibercrime «com um único clique», em que é possível seguir uma ligação que abre instantaneamente uma mensagem de correio eletrónico dirigida às autoridades competentes.

Na SE, certos tipos de crimes, como a fraude envolvendo cartões de crédito, também podem ser comunicados através do serviço eletrónico da Autoridade Policial. Além disso, os intervenientes nas atividades bancárias e de financiamento estão obrigados a comunicar à autoridade policial as atividades suspeitas relacionadas com potenciais casos de branqueamento de capitais ou de financiamento do terrorismo, ou os bens provenientes de outros atos criminosos. Além disso, é mantido um diálogo permanente entre as operações bancárias e financeiras e o Centro Nacional de Luta contra a Fraude da Autoridade Policial.

As disposições jurídicas da SK estabelecem o dever (e os procedimentos) de as autoridades públicas e outras pessoas coletivas comunicarem imediatamente as infrações penais às autoridades responsáveis pela aplicação da lei. Existem também obrigações de comunicação relativas ao branqueamento de capitais por parte das pessoas obrigadas e, especificamente, dos bancos.

Em alternativa, nos NL e na PL foram tomadas medidas não legislativas para aplicar o artigo 15.º da diretiva. As linhas telefónicas e o sítio Web da Polícia Neerlandesa constituem um canal adequado para comunicar às autoridades os casos de fraude que envolvam meios de pagamento que não em numerário. Além disso, o governo neerlandês comprometeu-se a encorajar as instituições financeiras e outras pessoas coletivas a comunicar qualquer suspeita de fraude. Este esforço é visível, por exemplo, na existência de um gabinete de atendimento para a fraude financeira instalado em todas as unidades policiais dos Países Baixos. Além disso, quatro grandes bancos e a empresa ICS assinaram um acordo com a polícia para combater a fraude (bancária) e a ciberiscagem em conjunto. Na PL, as denúncias de crimes são aceites 24 horas por dia, sete dias por semana, por todas as unidades policiais. Além disso, devido à natureza dos crimes cometidos com recurso a tecnologias informáticas, é possível contactá-las diretamente através de uma unidade organizacional especializada da Direção-Geral da Polícia. Ademais, a fim de assegurar a mais rápida cooperação possível com o setor bancário, foi estabelecido um canal de cooperação entre o Gabinete de Combate à Cibercriminalidade da Direção-Geral da Polícia e o Centro de Segurança Bancária da Associação Bancária Polaca.

O artigo 15.º, n.º 2, da diretiva não foi transposto na BG, EE e HR.

2.5 Apoio às vítimas e prevenção

a) Assistência e apoio às vítimas

A assistência e o apoio às pessoas singulares e coletivas cujos dados pessoais tenham sido utilizados indevidamente são garantidos pelo artigo 16.º, n.º 1 da diretiva. As medidas devem incluir: a) a disponibilização de informações e aconselhamento específicos sobre a proteção contra as consequências negativas de tais crimes; e b) o fornecimento de uma lista de instituições especializadas que lidam com os diferentes aspetos dos crimes relacionados com a identidade e com a prestação de apoio às vítimas.

Na mesma linha, as pessoas coletivas vítimas dos crimes referidos nos artigos 3.º a 8.º da diretiva devem ter acesso a informações sobre: a) os procedimentos para apresentação de denúncias; b) o direito a receber informações sobre o processo; c) os procedimentos existentes para apresentação de denúncias caso a autoridade competente não respeite os direitos das vítimas no decurso do processo penal; e d) os contactos para o envio de comunicações relativas ao seu processo (artigo 16.º, n.º 3, da diretiva).

O Código de Processo Penal da maior parte dos Estados-Membros contém disposições sobre a vítima e os seus direitos, incluindo algumas disposições específicas sobre o direito da vítima à informação e a assistência durante o processo, o direito ao aconselhamento e o direito a apresentar queixa. Uma lei específica de transposição da diretiva complementa frequentemente o que já figura no Código de Processo Penal. As pessoas coletivas são geralmente objeto de disposições jurídicas distintas no Código de Processo Penal, ou outro. Além disso, existem várias campanhas de informação, folhetos, sítios Web específicos, circulares, etc., para ajudar e apoiar as vítimas dos crimes referidos nos artigos 3.º a 8.º da diretiva. É o caso na AT, BE (no que respeita ao artigo 16.º, n.º 1), CY, CZ, DE, IT, LT, LU (no que respeita ao artigo 16.º, n.º 1), LV (no que respeita ao artigo 16.º, n.º 3), RO, SI (no que respeita ao artigo 16.º, n.º 3), EE, FI (no que respeita ao artigo 16.º, n.º 1), FR (no que respeita ao artigo 16.º, n.º 1), HR, HU, NL, PL (no que respeita ao artigo 16.º, n.º 3), PT, SE e SK. O artigo 16.º, n.º 1, e/ou o artigo 16.º, n.º 3, da diretiva nunca foram transpostos literalmente ou quase literalmente, com exceção de MT.

A lista dos serviços de aconselhamento acreditados que prestam assistência às vítimas, referida no artigo 16.º, n.º 1, alínea b), da diretiva, está geralmente disponível em linha, pelo que é aplicada na prática.

b) Prevenção

O artigo 17.º, relativo à prevenção, exige que os Estados-Membros tomem as medidas adequadas, como, por exemplo, campanhas de informação e sensibilização, e programas de investigação e educação. A presente secção baseia-se numa avaliação das informações notificadas pelos Estados-Membros à Comissão, bem como numa pesquisa de fonte aberta na Internet para determinar a existência de medidas de prevenção. Tal como descrito no Quadro 2, quando foram identificadas ações de prevenção, estas referem-se principalmente à cibercriminalidade e à fraude em linha. No entanto, em alguns países, são também fornecidas informações sobre a prevenção da fraude, geralmente pela polícia.

Quadro 2 Ações de prevenção

EM	Ações
AT	A Polícia Federal fornece regularmente informações no seu sítio Web e nas redes sociais sobre as formas de se proteger contra a fraude. A cooperação com as partes interessadas, como a Câmara de Comércio, é apoiada e implementada no âmbito de projetos de comércio eletrónico.
BE	Diferentes sítios Web com materiais de aconselhamento/sensibilização, como os geridos pelo Centro de Cibersegurança da Bélgica (CCB). Através de pesquisa na Internet foi possível identificar algumas medidas de cooperação com as partes interessadas, por exemplo, a organização que representa o setor financeiro cooperou com a Procuradoria de Bruxelas (*Parquet*) para desenvolver materiais de sensibilização
BG	Em 2021, teve início uma campanha de luta contra as «mulas financeiras» na Bulgária, dirigida pela Associação de Bancos e levada a cabo em conjunto com a Direção-Geral «Luta contra a Criminalidade Organizada» e o Ministério Público. A Direção-Geral lançou igualmente uma campanha sobre ciberiscagem.
CY	A Subdivisão de Cibercrime da Polícia disponibiliza no seu sítio Web informações e conselhos sobre questões como a fraude digital, bem como informações sobre eventos futuros como, por exemplo,

	campanhas de sensibilização. Um exemplo é a campanha de informação sobre segurança da informação levada a cabo pela Polícia, pelos Bancos Centrais, pela Associação de Bancos e pela Autoridade de Segurança Digital.
DE	A Polícia Federal (BKA) disponibiliza no seu sítio Web uma panorâmica das medidas destinadas à parceria público-privada institucionalizada para efeitos de deteção, prevenção, investigação ou repressão das infrações abrangidas pela diretiva como, por exemplo, a parceria entre o Serviço Federal de Polícia Judiciária (BKA), o Serviço Federal de Segurança da Informação (BSI) e o Centro Alemão de Competência contra a Cibercriminalidade e.V. (G4C), uma associação de instituições financeiras e de empresas do setor da segurança informática. O BKA lançou também a Conferência sobre Cibercriminalidade C³, uma plataforma de intercâmbio entre autoridades, empresas, o mundo científico e os responsáveis políticos. O G4C também produz brochuras informativas e organiza ações de formação. Por último, o BKA participa igualmente na elaboração de medidas de prevenção no domínio da cibercriminalidade a nível dos Länder . A nível nacional, o BKA também está ligado em rede com outras autoridades e organizações policiais e não policiais (partes interessadas) e está a intensificar a cooperação, em especial em temas da atualidade.
FR	O Ministério do Interior publica informações sobre a prevenção em matéria de cibercriminalidade. As plataformas disponíveis para denunciar o cibercrime incluem também mensagens de prevenção, tal como o Serviço de Informação e Comunicação da Polícia Nacional (SICoP). Outros exemplos incluem as orientações emitidas pelo Banco de França ou o guia sobre a prevenção da fraude publicado pelo grupo de trabalho nacional de luta contra a fraude, que agrupa diferentes autoridades administrativas e de aplicação da lei.
EL	A Divisão de Cibercrime e a Direção-Geral da Polícia são muito ativas na informação do público, na sensibilização e na redução do risco de se tornar vítima de fraude, recorrendo a campanhas televisivas, discursos de cariz pedagógico e informações em linha.
ES	O Instituto Nacional de Cibersegurança Espanhol e a Autoridade Tributária disponibilizam no seu sítio Web informações relevantes para prevenir a ciberiscagem, o *software de sequestro*, etc., em ambientes profissionais.
HR	O Ministério do Interior fornece informações em linha sobre as fraudes na Internet e gere um canal no YouTube dedicado à fraude e à segurança informática, com vídeos sobre fraudes cibernéticas.
IT	O Ministério do Tesouro, que tem por missão prevenir a fraude sobre os meios de pagamento, promove já uma série de iniciativas a nível local, em colaboração com as administrações locais e o mundo académico, organizando seminários e sessões de trabalho dirigidos às categorias afetadas pela contrafação de moeda, incluindo os cidadãos.
LT	Estão disponíveis informações sobre prevenção da fraude em linha no sítio Web da Autoridade Reguladora das Comunicações, enquanto o sítio Web da Polícia contém informações sobre os tipos mais comuns de ciberfraude. Além disso, um dos objetivos da Estratégia Nacional para a Cibercriminalidade é reforçar a prevenção e o controlo da cibercriminalidade, em especial através do desenvolvimento de uma cooperação eficaz entre as autoridades responsáveis pela aplicação da lei e outras partes interessadas.
LV	A Comissão dos Mercados Financeiros e dos Capitais desenvolveu várias ferramentas na Internet para fornecer informações e orientações sobre questões de segurança financeira e fraude. Além disso, foram organizadas várias campanhas em cooperação com a Polícia Nacional e o Centro de Proteção dos Direitos do Consumidor.
NL	Estão a ser tomadas medidas, como a «Fraudehelpdesk» (linha de apoio para casos de fraude), uma organização subsidiada pelo governo neerlandês. A *Fraudehelpdesk* faz parte da «SAFECIN stichting» (Fundação para a luta contra a criminalidade financeira e económica nos Países Baixos), uma fundação com participação governamental.
SE	É mantido um diálogo permanente entre as operações bancárias e financeiras e o Centro Nacional de Luta contra a Fraude da Autoridade Policial, NBC. Além disso, o NBC colabora, também para efeitos de prevenção da criminalidade, por exemplo, com intervenientes do comércio eletrónico. Nestes contactos, é sublinhada a importância de denunciar a fraude à polícia.

Em dez Estados-Membros (CZ, EE, FI, HU, MT, PL, PT, RO, SI e SK) não foram encontradas informações sobre ações de prevenção adequadas e a sua aplicação prática, embora em MT e RO a legislação reflita esta obrigação, seguindo de perto a redação da diretiva.

3. Conclusões e próximas etapas

A diretiva conduziu a progressos substanciais na criminalização da fraude e da contrafação de meios de pagamento que não em numerário a um nível comparável em todos os Estados-Membros, o que facilita a cooperação transfronteiras das autoridades responsáveis pela aplicação da lei que investigam este tipo de infrações. Os Estados-Membros alteraram os respetivos códigos penais e demais legislações aplicáveis, aplicaram procedimentos simplificados e criaram ou melhoraram os seus programas de cooperação. A Comissão reconhece os esforços significativos envidados pelos Estados-Membros para transpor a diretiva.

Contudo, ainda existe margem para a diretiva atingir todo o seu potencial, se os Estados-Membros aplicarem plenamente todas as suas disposições. A análise efetuada até à data sugere que algumas das principais melhorias a realizar pelos Estados-Membros dizem respeito ao artigo 2.º, alínea d), que estabelece a definição de moeda virtual; ao artigo 7.º, relativo aos instrumentos utilizados para cometer infrações, e ao artigo 8.º, n.º 2, relativo à tentativa; ao artigo 9.º, n.º 6, relativo às sanções penais aplicáveis às pessoas singulares no caso de a infração ser cometida no contexto de uma organização criminosa; ao artigo 14.º, relativo ao intercâmbio de informações; e ao artigo 16.º, relativo à assistência e apoio às vítimas.

A Comissão continuará a apoiar os Estados-Membros na aplicação da diretiva. Em particular, será publicado um convite à apresentação de propostas específico em 2023.

A Comissão está empenhada em velar pela conclusão da transposição em toda a UE e pela correta aplicação das disposições. Tal implica assegurar que as medidas nacionais são conformes com as disposições correspondentes da diretiva. Sempre que necessário, a Comissão exercerá os poderes de execução que lhe são conferidos pelos Tratados, através de processos por infração.