Conselho da
União Europeia

Bruxelas, 14 de setembro de 2017
(OR. en)

12181/17

Dossiê interinstitucional:
2017/0226 (COD)

DROIPEN 120
CYBER 126
JAI 784
TELECOM 206
MI 626
IA 138
CODEC 1400

PROPOSTA

de:	Secretário-Geral da Comissão Europeia, assinado por Jordi AYET PUIGARNAU, Diretor
data de receção:	13 de setembro de 2017
para:	Jeppe TRANHOLM-MIKKELSEN, Secretário-Geral do Conselho da União Europeia
n.° doc. Com.:	COM(2017) 489 final
Assunto:	Proposta de DIRETIVA DO PARLAMENTO EUROPEU E DO CONSELHO 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(2017) 489 final.

Anexo: COM(2017) 489 final

COMISSÃO
EUROPEIA

Bruxelas, 13.9.2017
COM(2017) 489 final

2017/0226 (COD)

Proposta de

DIRETIVA DO PARLAMENTO EUROPEU E DO CONSELHO

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

{SWD(2017) 298 final}
{SWD(2017) 299 final}

ÍNDICE

EXPOSIÇÃO DE MOTIVOS

1. CONTEXTO DA PROPOSTA

1.1. Justificação e objetivos da proposta

A atual legislação da UE que prevê regras mínimas comuns para criminalizar a fraude de meios de pagamento que não em numerário é a Decisão-Quadro 2001/413/JAI do Conselho, de 28 de maio de 2001, relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário[1].

A Agenda Europeia para a Segurança[2] reconhece que a decisão-quadro já não reflete as realidades dos nossos dias e que dá uma resposta insuficiente aos novos desafios e avanços tecnológicos, tais como as moedas virtuais e os pagamentos móveis.

Em 2013, as fraudes cometidas utilizando cartões emitidos no espaço único de pagamentos em euros (SEPA) totalizaram 1,44 mil milhões de EUR, representando um aumento de 8 % face ao ano anterior. Embora os dados disponíveis sobre fraude digam apenas respeito aos pagamentos com cartões, os cartões constituem o instrumento de pagamento que não em numerário mais importante na UE em termos de número de transações[3].

É importante dar uma resposta efetiva à fraude de meios de pagamento que não em numerário, uma vez que esta representa uma ameaça à segurança. A fraude de meios de pagamento que não em numerário constitui um rendimento para a criminalidade organizada e, como tal, potencia outras atividades criminosas, tais como o terrorismo, o tráfico de estupefacientes e o tráfico de seres humanos. Mais concretamente, de acordo com a Europol, a fraude de meios de pagamento que não em numerário é utilizada para financiar:

- Viagens:
    - voos: a experiência adquirida com a realização das operações do «Global Airline Action Day»[4] de 2014 a 2016 revela que existe uma ligação clara entre a fraude de meios de pagamento que não em numerário, a fraude com bilhetes de avião e outros crimes graves e organizados, incluindo o terrorismo. Verificou-se que algumas das pessoas que viajaram com bilhetes obtidos de forma fraudulenta estavam envolvidas, ou havia suspeitas do seu envolvimento, noutras infrações;
    - outras fraudes relacionadas com viagens (ou seja, vender ou viajar com bilhetes obtidos de forma fraudulenta). A compra de bilhetes ilegais faz-se principalmente através da utilização de cartões de crédito comprometidos. Outros métodos incluem a utilização de contas de pontos de fidelidade comprometidas, agências de viagens para *phishing* e fraude com *vouchers*.

---

1 Jornal Oficial L 149 de 2.6.2001, p. 1.

2 Comunicação da Comissão *Estratégia para o Mercado Único Digital na Europa*, COM(2015) 192 final.

3 Banco Central Europeu, *Quarto relatório sobre fraude com cartões*, julho de 2015 (dados disponíveis mais recentes)

4 Mais informações aqui.

Além dos criminosos, viajam com bilhetes obtidos de forma fraudulenta as pessoas vítimas de tráfico e os internautas que lavam dinheiro[5].

- Alojamento: as autoridades policiais comunicam igualmente que a fraude de meios de pagamento que não em numerário também é utilizada para facilitar outros crimes que exigem alojamento temporário, como acontece com o tráfico de seres humanos, a imigração ilegal e o tráfico de estupefacientes.

A Europol também comunicou que o mercado do crime na UE no que toca à fraude de pagamento com cartões é dominado por grupos da criminalidade organizada bem estruturados e ativos a nível global[6].

Além disso, a fraude de meios de pagamento que não em numerário dificulta o desenvolvimento do mercado único digital de duas formas:

- causa perdas económicas diretas significativas, como indica o nível estimado de fraude com cartões de 1,44 mil milhões de EUR supramencionado. Por exemplo, as companhias aéreas perdem globalmente cerca de mil milhões de USD por ano com a fraude com cartões[7];

- reduz a confiança dos consumidores, o que pode resultar numa redução da atividade económica e numa participação limitada no mercado único digital. De acordo com o mais recente Eurobarómetro sobre Cibersegurança[8], os utilizadores da Internet, na sua grande maioria (85 %), consideram que o risco de se tornarem vítimas de cibercrime está a aumentar. Ademais, 42 % dos utilizadores estão preocupados com a segurança dos pagamentos em linha. Devido a estas preocupações com a segurança, a probabilidade de efetuarem transações digitais é menor para 12 % dos utilizadores.

Uma avaliação do atual quadro legislativo da UE[9] identificou três problemas que estão a impulsionar a atual situação em relação à fraude de meios de pagamento que não em numerário na UE:

1. Alguns crimes não podem ser **investigados e reprimidos eficazmente** ao abrigo do atual quadro jurídico.

2. Alguns crimes não podem ser investigados e reprimidos eficazmente devido a obstáculos operacionais.

3. Os criminosos aproveitam-se das lacunas existentes na **prevenção** para cometer fraudes.

---

5 O termo «agir na qualidade de internauta que lava dinheiro» indica uma pessoa que transfere produtos do crime entre diferentes países. Os internautas que lavam dinheiro recebem os produtos do crime nas suas contas, sendo-lhes então pedido que os levantem e os transfiram para uma conta diferente, frequentemente no estrangeiro, ficando com algum do dinheiro para si.

6 Europol, *Situation Report: Payment Card Fraud in the European Union*, 2012.

7 IATA, 2015.

8 Comissão Europeia, *Eurobarómetro especial 423* — *Cibersegurança*, fevereiro de 2015.

9 Documento de trabalho dos serviços da Comissão — Avaliação de impacto que acompanha a proposta de diretiva relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário, SWD(2017) 298.

A presente proposta tem três objetivos específicos para dar resposta aos problemas identificados:

1. Assegurar a existência de uma política/quadro jurídico claro, sólido e **tecnologicamente neutro**.

2. Eliminar os **obstáculos operacionais** que dificultam a investigação e a ação judicial.

3. Reforçar a **prevenção**.

1.2. Necessidade de aplicar as normas e obrigações internacionais pertinentes e de combater a fraude e a contrafação de meios de pagamento que não em numerário de forma eficaz

A Convenção do Conselho da Europa sobre a Criminalidade Informática (Convenção de Budapeste)[10], no seu título 2, que incide sobre as infrações relacionadas com a informática, exige que as partes na convenção definam a falsificação relacionada com a informática (artigo 7.º) e a fraude relacionada com a informática (artigo 8.º) como infrações penais ao abrigo das respetivas legislações nacionais. A decisão-quadro atualmente em vigor cumpre estas disposições. Fazer a revisão das atuais normas permitirá melhorar ainda mais a cooperação entre as autoridades policiais e judiciais e entre a polícia e as entidades privadas, contribuindo desta forma para o cumprimento dos objetivos globais da convenção, mantendo-se coerente com as suas disposições pertinentes.

1.3. Coerência com as disposições existentes no mesmo domínio setorial

Os objetivos da presente proposta são coerentes com a política e as disposições legislativas no domínio do direito penal apresentadas a seguir:

1. **Mecanismos de cooperação** pan-europeus **em matéria penal** que facilitam a coordenação da investigação e da ação judicial (direito penal processual):

   - Decisão-Quadro 2002/584/JAI do Conselho relativa ao mandado de detenção europeu e aos procedimentos de entrega entre Estados-Membros[11];

   - Convenção relativa ao auxílio judiciário mútuo em matéria penal entre os Estados-Membros da União Europeia[12];

   - Diretiva 2014/41/UE relativa à decisão europeia de investigação em matéria penal[13];

   - Decisão-Quadro 2005/214/JAI do Conselho relativa à aplicação do princípio do reconhecimento mútuo às sanções pecuniárias[14];

---

10 Convenção do Conselho da Europa sobre a Criminalidade Informática (STE n.º 185).

11 Decisão-Quadro 2002/584/JAI do Conselho, de 13 de junho de 2002, relativa ao mandado de detenção europeu e aos processos de entrega entre os Estados-Membros.

12 Ato do Conselho, de 29 de maio de 2000, que estabelece, em conformidade com o artigo 34.º do Tratado da União Europeia, a Convenção relativa ao auxílio judiciário mútuo em matéria penal entre os Estados-Membros da União Europeia.

13 Diretiva 2014/41/UE do Parlamento Europeu e do Conselho, de 3 de abril de 2014, relativa à decisão europeia de investigação em matéria penal

- Decisão-Quadro 2009/948/JAI do Conselho relativa à prevenção e resolução de conflitos de exercício de competência em processo penal[15];

- Decisão-Quadro 2009/315/JAI do Conselho relativa à organização e ao conteúdo do intercâmbio de informações extraídas do registo criminal entre os Estados-Membros[16];

- Diretiva 2012/29/UE que estabelece normas mínimas relativas aos direitos, ao apoio e à proteção das vítimas da criminalidade[17];

- Regulamento (UE) 2016/794 que cria a Europol[18];

- Decisão do Conselho 2002/187/JAI relativa à criação da Eurojust[19];

- Conclusões do Conselho sobre a melhoria da justiça penal no ciberespaço[20].

Por princípio, a presente proposta não introduz disposições específicas à fraude de meios de pagamento que não em numerário que não se coadunem com estes instrumentos mais abrangentes, com vista a evitar a fragmentação, algo que poderia complicar a transposição e a aplicação por parte dos Estados-Membros. A única exceção é a Diretiva 2012/29/UE que estabelece normas mínimas relativas aos direitos, ao apoio e à proteção das vítimas da criminalidade, que a presente proposta complementa.

2. Atos jurídicos que **criminalizam a prática** relacionada com a fraude e a contrafação de meios de pagamento que não em numerário (direito penal material):

- Diretiva 2013/40/UE relativa a ataques contra os sistemas de informação[21]:

  - a presente proposta complementa a Diretiva 2013/40/UE, uma vez que aborda um aspeto diferente da cibercriminalidade[22]. Os dois instrumentos

---

14 Decisão-Quadro 2005/214/JAI do Conselho, de 24 de fevereiro de 2005, relativa à aplicação do princípio do reconhecimento mútuo às sanções pecuniárias.

15 Decisão-Quadro 2009/948/JAI do Conselho, de 30 de novembro de 2009, relativa à prevenção e resolução de conflitos de exercício de competência em processo penal.

16 Decisão-Quadro 2009/315/JAI do Conselho, de 26 de fevereiro de 2009, relativa à organização e ao conteúdo do intercâmbio de informações extraídas do registo criminal entre os Estados-Membros.

17 Diretiva 2012/29/UE do Parlamento Europeu e do Conselho, de 25 de outubro de 2012, que estabelece normas mínimas relativas aos direitos, ao apoio e à proteção das vítimas da criminalidade e que substitui a Decisão-Quadro 2001/220/JAI do Conselho.

18 Regulamento (UE) 2016/794 do Parlamento Europeu e do Conselho, de 11 de maio de 2016, que cria a Agência da União Europeia para a Cooperação Policial (Europol) e que substitui e revoga as Decisões 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI e 2009/968/JAI do Conselho

19 Decisão 2002/187/JAI do Conselho, de 28 de fevereiro de 2002, relativa à criação da Eurojust a fim de reforçar a luta contra as formas graves de criminalidade.

20 Conclusões do Conselho, de 6 de junho de 2016, sobre a melhoria da justiça penal no ciberespaço.

21 Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho.

22 A estratégia da União Europeia para a cibersegurança indica que «[a] cibercriminalidade refere-se, geralmente, a um amplo leque de diferentes atividades criminosas que envolvem os computadores e os sistemas informáticos, quer como instrumentos quer como alvos principais. A cibercriminalidade inclui as infrações tradicionais (por exemplo, fraude, falsificação e roubo de identidade), infrações relativas aos conteúdos (por exemplo, distribuição de material pedopornográfico em linha ou incitamento ao ódio

correspondem a diferentes conjuntos de disposições da Convenção de Budapeste do Conselho da Europa sobre a Criminalidade Informática[23], que representa o quadro jurídico internacional de referência para a UE[24].

- a presente proposta também é coerente com a Diretiva 2013/40/UE, uma vez que tem por base uma abordagem idêntica em relação a questões específicas como competência jurisdicional e definição de níveis mínimos para as penas máximas.

- Diretiva 2014/62/UE relativa à proteção penal do euro e de outras moedas contra a contrafação[25]:

  - a presente proposta complementa a Diretiva 2014/62/UE, uma vez que abrange a contrafação de meios de pagamento que não em numerário, enquanto a Diretiva 2014/62/UE abrange a contrafação de numerário;

  - também é coerente com a Diretiva 2014/62/UE, uma vez que utiliza a mesma abordagem nalgumas disposições, como por exemplo nos instrumentos de investigação.

- Diretiva 2017/541/UE relativa à luta contra o terrorismo:

  - a presente proposta complementa a Diretiva 2017/541/UE, uma vez que pretende reduzir o montante global de fundos obtidos com fraudes de meios de pagamento que não em numerário, a maior parte dos quais são utilizados pelos grupos da criminalidade organizada para cometer crimes, incluindo terrorismo.

- Proposta de diretiva relativa ao combate ao branqueamento de capitais através do direito penal:

  - a presente proposta e a proposta de diretiva relativa ao combate ao branqueamento de capitais através do direito penal são complementares, uma vez que esta última institui o quadro jurídico necessário para combater o branqueamento dos produtos do crime gerados pela fraude de meios de pagamento que não em numerário (internautas que lavam dinheiro) como infração subjacente.

---

racial) e crimes respeitantes exclusivamente a computadores e sistemas informáticos (por exemplo, ataques contra os sistemas informáticos, recusa de serviço e software malicioso).»

23 Convenção do Conselho da Europa sobre a Criminalidade Informática (STE n.º 185). A Diretiva 2013/40/UE corresponde aos artigos 2.º a 6.º da Convenção, ao passo que uma nova iniciativa corresponderia aos artigos 7.º e 8.º da Convenção.

24 Comissão e Alta Representante da União Europeia para os Negócios Estrangeiros e a Política de Segurança — comunicação conjunta intitulada «Estratégia da União Europeia para a Cibersegurança: um ciberespaço aberto, seguro e protegido».

25 Diretiva 2014/62/UE do Parlamento Europeu e do Conselho, de 15 de maio de 2014, relativa à proteção penal do euro e de outras moedas contra a contrafação e que substitui a Decisão-Quadro 2000/383/JAI do Conselho.

1.4. Coerência com outras políticas da UE

A presente proposta é coerente com a Agenda Europeia para a Segurança e com a Estratégia da União Europeia para a Cibersegurança, uma vez que estas têm como principal objetivo aumentar a segurança.

Além disso, a presente proposta é coerente com a Estratégia para o Mercado Único Digital, que procura aumentar a confiança dos utilizadores no mercado digital, outro dos principais objetivos da proposta. No contexto da Estratégia para o Mercado Único Digital, existem vários instrumentos jurídicos que visam facilitar os pagamentos seguros da UE com os quais a presente proposta também é coerente:

- A Diretiva Serviços de Pagamento revista (DSP2)[26] contém várias medidas que reforçarão os requisitos de segurança aplicáveis aos pagamentos eletrónicos e constituirão um quadro jurídico e de supervisão para os novos participantes no mercado de pagamentos.

- A Diretiva 2015/849 relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo[27], (a quarta Diretiva Antibranqueamento de Capitais) abrange a situação em que os criminosos se aproveitam abusivamente dos instrumentos de pagamento que não em numerário para encobrir as suas atividades. A presente proposta complementa-a ao dar resposta à situação em que os instrumentos de pagamento que não em numerário tenham sido, por exemplo, ilicitamente apropriados, contrafeitos ou falsificados por criminosos.

- A proposta de diretiva que altera a Diretiva 2015/849 relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo[28], à qual a presente proposta vai buscar a mesma definição de moedas virtuais. Caso esta definição seja alterada durante o processo de adoção da referida proposta, a definição que consta a presente proposta deve passar a estar em consonância com a mesma.

- Outros atos jurídicos pertinentes incluem o Regulamento (UE) 2015/847 relativo às informações que acompanham as transferências de fundos[29]; o Regulamento (UE) n.º 910/2014 relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno[30]; o Regulamento (UE) n.º 260/2012 que

---

26 Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, relativa aos serviços de pagamento no mercado interno, que altera as Diretivas 2002/65/CE, 2009/110/CE e 2013/36/UE e o Regulamento (UE) n.º 1093/2010, e que revoga a Diretiva 2007/64/CE.

27 Diretiva (UE) 2015/849 do Parlamento Europeu e do Conselho, de 20 de maio de 2015, relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo, que altera o Regulamento (UE) n.º 648/2012 do Parlamento Europeu e do Conselho, e que revoga a Diretiva 2005/60/CE do Parlamento Europeu e do Conselho e a Diretiva 2006/70/CE da Comissão.

28 Proposta de diretiva do Parlamento Europeu e do Conselho que altera a Diretiva (UE) 2015/849 relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo e que altera a Diretiva 2009/101/CE.

29 Regulamento (UE) 2015/847 do Parlamento Europeu e do Conselho, de 20 de maio de 2015, relativo às informações que acompanham as transferências de fundos e que revoga o Regulamento (CE) n.º 1781/2006.

30 Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE.

estabelece requisitos técnicos e de negócio para as transferências a crédito e os débitos diretos em euros[31]; e a Diretiva (UE) 2016/1148 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (Diretiva SRI)[32].

Em geral, estes atos jurídicos ajudam a instituir medidas preventivas mais fortes. A presente proposta complementa-os, uma vez que acrescenta medidas que impõem sanções à atividade criminosa e permitem intentar ações judiciais sempre que a prevenção falhe.

2. BASE JURÍDICA, SUBSIDIARIEDADE E PROPORCIONALIDADE

2.1. Base jurídica

A base jurídica da ação da UE é o artigo 83.º, n.º 1, do Tratado sobre o Funcionamento da União Europeia, que refere explicitamente a **contrafação de meios de pagamento**, a **criminalidade informática** e a **criminalidade organizada** como domínios de criminalidade particularmente grave com dimensão transfronteiriça:

«O Parlamento Europeu e o Conselho, por meio de diretivas adotadas de acordo com o processo legislativo ordinário, podem estabelecer regras mínimas relativas à definição das infrações penais e das sanções em domínios de ***criminalidade particularmente grave com dimensão transfronteiriça*** *que resulte da natureza ou das incidências dessas infrações, ou ainda da especial necessidade de as combater, assente em bases comuns.*

São os seguintes os domínios de criminalidade em causa: terrorismo, tráfico de seres humanos e exploração sexual de mulheres e crianças, tráfico de droga e de armas, branqueamento de capitais, corrupção, ***contrafação de meios de pagamento, criminalidade informática e criminalidade organizada****...»*

2.2. Geometria variável

A Decisão-Quadro 2001/413/JAI relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário é aplicável a todos os Estados-Membros.

Em conformidade com o Protocolo n.º 21 relativo à posição do Reino Unido e da Irlanda em relação ao espaço de liberdade, segurança e justiça, anexo aos Tratados, estes Estados-Membros podem decidir participar na adoção da presente proposta. Caso não o façam, mantêm a possibilidade de participar na aplicação da decisão mesmo após a sua adoção.

Uma vez que o Reino Unido notificou, em 29 de março de 2017, a sua intenção de abandonar a União, ao abrigo do artigo 50.º do Tratado da União Europeia (TUE), os Tratados deixarão de ser aplicáveis ao Reino Unido a partir da data da entrada em vigor do acordo de saída ou, na falta deste, dois anos após a notificação, a menos que o Conselho Europeu, em acordo com o Reino Unido, decida prorrogar esse prazo. Consequentemente, e sem prejuízo das

---

31 Regulamento (UE) n.º 260/2012 do Parlamento Europeu e do Conselho, de 14 de março de 2012, que estabelece requisitos técnicos e de negócio para as transferências a crédito e os débitos diretos em euros e que altera o Regulamento (CE) n.º 924/2009.

32 Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.

disposições do acordo de saída, a referida descrição da participação do Reino Unido na presente proposta só é aplicável até que o Reino Unido deixe de ser Estado-Membro.

Em conformidade com o Protocolo n.º 22 relativo à posição da Dinamarca, a Dinamarca não participa na adoção pelo Conselho das medidas relativas ao título V do TFUE (com exceção da política de vistos). Por conseguinte, de acordo com as disposições atualmente em vigor, a Dinamarca não participa na adoção da presente proposta, nem fica por ela vinculada.

2.3. Subsidiariedade

A fraude de meios de pagamento que não em numerário tem uma dimensão transfronteiriça muito importante, tanto dentro como fora da UE. Um exemplo típico pode envolver a cópia (*skimming*) dos dados de um cartão num país da UE, a criação de um cartão contrafeito com os dados copiados e o levantamento de dinheiro com o cartão contrafeito fora da UE, com vista a contornar as exigentes normas de segurança. Cada vez mais se verifica que estes crimes acontecem totalmente em linha.

Por conseguinte, o objetivo de combater eficazmente este tipo de crimes não pode ser suficientemente alcançado pelos Estados-Membros se agirem de forma isolada ou não coordenada:

- estes crimes criam situações em que a vítima, o autor da infração e as provas podem estar todos abrangidos por quadros jurídicos nacionais diferentes dentro e fora da UE. Consequentemente, pode ser demasiado moroso e difícil para os países combaterem eficazmente estas atividades criminosas sem regras mínimas comuns;

- a necessidade de uma ação ao nível da UE já foi reconhecida através da criação da atual legislação da UE que visa combater a fraude e a contrafação de meios de pagamento que não em numerário (a decisão-quadro);

- a necessidade de uma intervenção ao nível da UE também está refletida nas atuais iniciativas que visam coordenar as medidas dos Estados-Membros nesta matéria ao nível da UE, tais como uma equipa da Europol que se dedica especificamente à fraude de meios de pagamento[33] e a prioridade EMPACT do ciclo político relativa à cooperação operacional contra a fraude de meios de pagamento que não em numerário[34]. O valor acrescentado destas iniciativas que visam ajudar os Estados-Membros a combater estes crimes foi reconhecido várias vezes na consulta das partes interessadas aquando da preparação da presente proposta, especialmente durante as reuniões de peritos.

Outro valor acrescentado da ação ao nível da UE é facilitar a cooperação com países que não pertencem à UE, uma vez que a dimensão internacional da fraude de meios de pagamento que não em numerário ultrapassa as fronteiras da UE. A existência de regras comuns mínimas na UE também pode inspirar soluções legislativas eficazes nos países que não pertencem à UE, facilitando assim a cooperação transfronteiriça ao nível global.

---

33 Ver sítio Web da Europol.

34 Mais informações aqui.

2.4. Proporcionalidade

Em conformidade com o princípio da proporcionalidade, tal como consagrado no artigo 5.º, n.º 4, do TUE, a nova proposta de diretiva está limitada ao que é necessário e proporcionado para aplicar as normas internacionais e adaptar a legislação existente neste domínio às novas ameaças. A inclusão de medidas relacionadas com a utilização de instrumentos de investigação e com o intercâmbio de informações limitam-se ao que é necessário para um funcionamento eficaz do quadro penal proposto.

A proposta define o âmbito de aplicação das infrações penais por forma a abranger todos os comportamentos pertinentes, mas sem exceder o que é necessário e proporcionado.

2.5. Escolha do instrumento

Em conformidade com o artigo 83.º, n.º 1, do TFUE, o estabelecimento de regras mínimas relativas à definição das infrações penais e das sanções em domínios de criminalidade particularmente grave com dimensão transnacional, nos quais se inclui a contrafação de meios de pagamento e a criminalidade informática, só pode ser alcançado através de uma diretiva do Parlamento Europeu e do Conselho adotada de acordo com o processo legislativo ordinário.

3. RESULTADOS DAS AVALIAÇÕES EX POST, DA CONSULTA DAS PARTES INTERESSADAS E DAS AVALIAÇÕES DE IMPACTO

3.1. Avaliações ex post/balanços de qualidade da legislação em vigor

A Comissão realizou uma avaliação[35] do atual quadro legislativo da UE, juntamente com a avaliação de impacto que acompanha a presente proposta (para mais informações, consultar o correspondente documento de trabalho dos serviços da Comissão).

A avaliação detetou três problemas principais, cada um com várias subdivisões:

[35] Documento de trabalho dos serviços da Comissão — Avaliação de impacto que acompanha a proposta de diretiva relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário, SWD(2017) 298.

Principais problemas	Subdivisão dos problemas
1. Alguns crimes não podem ser **investigados e reprimidos eficazmente** ao abrigo do atual **quadro jurídico**.	a. Alguns crimes não podem ser reprimidos eficazmente porque as infrações cometidas com determinados instrumentos de pagamento (em especial os **não corpóreos**) estão criminalizadas de maneira diferente nos Estados-Membros ou não se encontram criminalizadas. b. Os **atos preparatórios** das fraudes com meios de pagamento que não em numerário não podem ser reprimidos eficazmente porque estão criminalizados de maneira diferente nos Estados-Membros ou não se encontram criminalizados. c. As investigações transfronteiriças podem ser prejudicadas porque algumas infrações são sancionadas com diferentes **níveis de sanções** nos Estados-Membros. d. As deficiências na atribuição da **competência jurisdicional** podem prejudicar a eficácia das investigações e das ações judiciais.
2. Alguns crimes não podem ser **investigados e reprimidos eficazmente** devido a **obstáculos operacionais**.	a. O fornecimento de informações quando existem pedidos de **cooperação transfronteiriça** pode ser demasiado moroso, o que prejudica as investigações e a ação judicial. b. A reduzida comunicação de informações às autoridades policiais devido aos constrangimentos existentes ao nível da **cooperação público-privada** prejudica a eficácia das investigações e das ações judiciais.
3. Os criminosos aproveitam-se das lacunas na **prevenção** para cometer fraudes.	a. As lacunas existentes ao nível da **partilha de informações** na **cooperação público-privada** prejudicam a prevenção. b. Os criminosos exploram a **falta de sensibilização** das vítimas.

Os principais problemas indicam que estamos sobretudo perante uma **deficiência regulamentar**, tendo em conta que o atual quadro legislativo da UE (a decisão-quadro) se tornou parcialmente obsoleto, devido principalmente aos **avanços tecnológicos**. A avaliação indicou que esta lacuna regulamentar não foi suficientemente colmatada pela legislação mais recente.

3.2. Consulta das partes interessadas

Atividades de consulta:

Foram realizados três tipos de atividades de consulta: consulta pública aberta, consulta orientada organizada pela Comissão Europeia e consulta orientada organizada por um contratante:

1. Consulta pública aberta

A Comissão Europeia lançou uma consulta pública aberta, em 1 de março de 2017, com o objetivo de recolher opiniões junto do público em geral relativamente à definição do problema, à pertinência e eficácia do atual quadro jurídico no domínio da fraude de meios de pagamento que não em numerário, bem como às opções e aos possíveis impactos destas para dar resposta às questões existentes. A consulta foi encerrada passadas 12 semanas, no dia 24 de maio de 2017.

Responderam aos questionários da consulta 33 profissionais e 21 membros do público em geral. Quatro profissionais deram o seu contributo por escrito. Os profissionais incluíam:

- empresas privadas (setor privado);
- autoridades internacionais ou nacionais (agências policiais, autoridades judiciais e instituições e organismos da UE);
- associações comerciais, empresariais ou profissionais (p. ex. federações bancárias nacionais);
- organizações, plataformas ou redes não governamentais;
- consultores profissionais, sociedades de advogados, consultores independentes.

2. Consulta orientada organizada pela Comissão Europeia:

- grandes reuniões de peritos com representantes das autoridades policiais e judiciais de todos os países da UE (selecionados pelos Estados-Membros) e peritos do setor privado (instituições financeiras, prestadores de serviços de pagamento, comerciantes, sistemas de cartões);
- várias reuniões com peritos e partes interessadas do mundo académico, de agências policiais, indústrias ligadas à moeda virtual, representantes de organizações de consumidores, representantes de instituições financeiras privadas e representantes de reguladores financeiros.

3. Consulta orientada organizada por um contratante:

Um contratante organizou consultas orientadas que incluíram inquéritos em linha e entrevistas. Os resultados preliminares foram apresentados a um grupo de validação, que posteriormente comunicou e verificou os resultados da consulta.

Globalmente, estiveram envolvidas 125 partes interessadas de 25 Estados-Membros.

Principais resultados:

- Dimensão da criminalidade:

  Os custos relacionados com a fraude de meios de pagamento que não em numerário são em geral percecionados como elevados e espera-se que aumentem nos próximos anos. As partes interessadas de todas as categorias sentiram dificuldades quando lhes foi pedido para quantificarem o fenómeno criminoso. As estatísticas são raras e nem sempre estão acessíveis. Contudo, algumas das partes interessadas forneceram dados baseados em casos concretos apontando para a relevância de certos tipos de fraude com meios de pagamento que não em numerário.

- Quadro penal:

  As partes interessadas, na sua maioria, consideraram que o atual quadro jurídico da UE é apenas parcialmente pertinente face às atuais necessidades de segurança, especialmente no que toca à definição de instrumentos de pagamento e infrações penais. Algumas confirmaram que os quadros jurídicos nacionais necessitariam de ser alterados.

- Direito penal processual:

  Não obstante o quadro jurídico existente, o nível atual de cooperação entre os Estados-Membros em termos de investigações e ações judiciais é percecionado como parcialmente satisfatório. O apoio da Europol com vista a facilitar a cooperação transfronteiriça foi amplamente reconhecido.

- Comunicação de informações às autoridades policiais:

  Os pontos de vista em relação à comunicação de informações às autoridades policiais diferiram: alguns mostraram-se satisfeitos com o nível atual de comunicação de informações, ao passo que outros acreditavam que deve ser melhorado. As diferentes categorias de partes interessadas concordaram quanto ao facto de as futuras opções políticas sobre comunicação de informações necessitarem de ser equilibradas com as capacidades atuais das autoridades policiais para fazer um acompanhamento dos processos.

- Cooperação entre os setores público e privado:

  As partes interessadas consideraram que a cooperação entre os setores público e privado foi globalmente benéfica e concordaram quanto ao facto de esta dever ser incentivada com vista a combater melhor a fraude com meios de pagamento que não em numerário, especialmente no que diz respeito à prevenção.

  Na sua maioria, as partes interessadas consideraram que a cooperação público-privada deve ser melhorada para combater a fraude de meios de pagamento que não em numerário. Os representantes do setor privado pareceram estar muito insatisfeitos. É perceção destes que os principais obstáculos à cooperação incluem, por exemplo, limitações na possibilidade de partilhar informações com as autoridades policiais e nas ferramentas conexas utilizadas para permitir este intercâmbio.

  A grande maioria das partes interessadas concorda que, por forma a investigar e julgar os criminosos, as instituições financeiras devem poder partilhar espontaneamente algumas informações pessoais das vítimas com a polícia nacional ou com a polícia de outro país da UE (p. ex. nome, conta bancária, morada, etc.).

  A má cooperação entre autoridades privadas e públicas também foi referida por várias partes interessadas como sendo um obstáculo à luta contra a fraude com meios de pagamento que não em numerário.

  A legislação, o não alinhamento das várias prioridades e a falta de confiança, juntamente com questões práticas e organizacionais, são encarados pelas empresas privadas, autoridades públicas, associações comerciais, empresariais e profissionais como obstáculos a uma cooperação bem-sucedida entre autoridades públicas e entidades privadas quando os participantes estão sediados em diferentes países da UE. A falta de tecnologia apropriada (p. ex. um canal de comunicações) também foi referida como um obstáculo por empresas privadas e autoridades públicas.

- Direitos das vítimas:

  As partes interessadas salientaram a importância de proteger as vítimas de fraude. Algumas consideraram que as vítimas não estão suficientemente protegidas, embora as iniciativas adotadas ao nível dos Estados-Membros para as proteger sejam globalmente valorizadas. As associações das vítimas desenvolveram bons mecanismos de cooperação com as autoridades policiais. Várias partes interessadas consideraram ser necessário proteger melhor as vítimas contra o roubo de identidade, que é percecionado como algo que afeta tanto as pessoas singulares como as pessoas coletivas. Por conseguinte, as vítimas devem ser protegidas independentemente da sua natureza jurídica.

3.3. Avaliação de impacto

De acordo com as Orientações para Legislar Melhor[36] da Comissão, a Comissão realizou uma avaliação de impacto[37] para aferir a necessidade de uma proposta legislativa.

A avaliação de impacto foi apresentada e debatida com o Comité de Controlo da Regulamentação (CCR) no dia 12 de julho de 2017. O comité reconheceu os esforços para quantificar os custos e os benefícios. Deu um parecer positivo[38], com a recomendação de se continuar a melhorar o relatório no que diz respeito aos seguintes aspetos:

1. O relatório não explicava suficientemente o contexto da política, nomeadamente a relação e a complementaridade dos mecanismos de cooperação judiciais e pan-europeus existentes e pretendidos.

2. O objetivo da iniciativa, relacionado com o crescimento, parecia sobrevalorizado.

O relatório da avaliação de impacto foi revisto tendo em conta as recomendações do comité que constam do seu parecer positivo.

Depois de identificadas as possíveis medidas políticas destinadas a dar resposta a cada um dos problemas identificados na avaliação e após analisar quais as medidas que deveriam ser mantidas e quais deveriam ser descartadas, as medidas foram agrupadas em opções políticas. Cada opção política foi concebida para dar resposta a todos os problemas identificados. As várias opções políticas consideradas são cumulativas, ou seja, apresentam um nível crescente de ação legislativa ao nível da UE. Dado que o problema em apreço se trata basicamente de uma **deficiência regulamentar**, foi importante apresentar todos os instrumentos regulamentares para determinar a resposta mais proporcionada ao nível da UE.

As diferentes opções consideradas foram:

- **opção A:** melhorar a aplicação da legislação da UE e facilitar a autorregulação para a cooperação público-privada;

---

36 Pode consultar mais informações sobre as Orientações da Comissão para Legislar Melhor aqui.

37 Documento de trabalho dos serviços da Comissão — Avaliação de impacto que acompanha a proposta de diretiva relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário, SWD(2017) 298.

38 Comité de Controlo da Regulamentação da Comissão Europeia — Parecer sobre a avaliação de impacto — Combater a fraude e a contrafação de meios de pagamento que não em numerário, SEC(2017)390.

- **opção B:** introduzir um novo quadro legislativo e facilitar a autorregulação para a cooperação público-privada;

- **opção C:** igual à opção B, mas com disposições que incentivem a comunicação de informações no âmbito da cooperação público-privada em vez da autorregulação, bem como novas disposições em matéria de sensibilização;

- **opção D:** igual à opção C, mas com disposições adicionais no domínio da competência jurisdicional que complementem a Decisão Europeia de Investigação e as regras relativas às injunções.

A opção C foi a opção preferida, tanto em termos qualitativos como em termos de custos e benefícios.

Em termos de benefícios, a opção preferida abriria caminho a uma ação policial mais eficaz e eficiente contra a fraude de meios de pagamento que não em numerário, através de uma aplicação mais coerente das regras em toda a UE, uma melhor cooperação transfronteiriça, uma cooperação público-privada mais sólida e um intercâmbio de informações mais reforçado. A iniciativa também fomentaria a confiança no mercado único digital através do reforço do segurança.

Em termos de custos, estima-se que os custos de criar e aplicar uma nova iniciativa para os Estados-Membros rondem os 561 000 EUR (verba única). Para os Estados-Membros, estima-se que os custos contínuos de aplicação e execução totalizem cerca de 2 285 140 EUR por ano (total para todos os Estados-Membros).

Como não estão previstas na proposta disposições que obriguem à apresentação de relatórios, não deve haver impacto no que diz respeito a custos adicionais para as empresas, incluindo PME. As outras disposições que seriam incluídas na proposta também não afetam as PME.

Globalmente, espera-se que o impacto cumulativo das medidas propostas nos custos administrativos e financeiros seja superior aos níveis atuais, uma vez que o número de casos a investigar colocaria sob pressão os recursos policiais neste domínio e estes teriam de ser aumentados. As principais razões para tal prendem-se com:

- o facto de ser provável que uma definição mais alargada dos meios de pagamento e um maior número de infrações às quais dar resposta (atos preparatórios) aumentem o número de casos pelos quais as autoridades policiais e judiciais são responsáveis;

- o facto de serem necessários recursos adicionais para intensificar a cooperação transfronteiriça;

- o facto de a obrigação que recai sobre os Estados-Membros de recolherem dados estatísticos criar um encargo administrativo adicional.

Por outro lado, a criação de um quadro jurídico claro destinado a travar os meios que facilitam a fraude de meios de pagamento que não em numerário constituiria uma oportunidade para detetar, agir judicialmente e sancionar as atividades fraudulentas numa fase precoce. Além disso, embora o reforço da cooperação público-privada tenha um custo em termos de recursos, o retorno do investimento em termos de eficácia e eficiência da ação policial é imediato.

3.4. Adequação e simplificação da legislação

Em termos qualitativos, a presente proposta tem potencial de simplificação nalguns domínios, como por exemplo:

- uma maior aproximação dos quadros penais nacionais (p. ex. estipulando definições comuns e um nível mínimo comum de sanções para as penas máximas) simplificaria e facilitaria a cooperação entre as agências policiais nacionais que investigam e agem judicialmente em casos transfronteiriços;

- em particular, a existência de regras mais claras sobre competência jurisdicional, um papel mais forte e reforçado dos pontos de contacto nacionais e a partilha de dados e informações entre as autoridades policiais nacionais e com a Europol poderia simplificar ainda mais os processos e as práticas no domínio da cooperação.

Não é possível quantificar o potencial de simplificação devido à falta de dados (e, em alguns casos, à impossibilidade de isolar os efeitos da decisão-quadro).

Globalmente, o potencial da presente iniciativa em termos de adequação regulamentar é muito limitado:

1. Em primeiro lugar, a decisão-quadro de 2001 já é um ato jurídico relativamente simples com potencial limitado de maior simplificação.

2. Em segundo lugar, a presente iniciativa tem como objetivo aumentar a segurança dando resposta às atuais lacunas. Regra geral, isto implicaria mais custos administrativos para investigar crimes que não se encontram atualmente abrangidos e agir judicialmente em relação aos mesmos, em vez de conseguir poupanças significativas resultantes da simplificação da cooperação transfronteiriça.

3. Em terceiro lugar, a iniciativa não pretende impor obrigações legais adicionais às empresas e aos cidadãos. Solicita aos Estados-Membros que incentivem e facilitem a comunicação de informações através de canais adequados (em vez de impor a comunicação de informações obrigatórias), em consonância com outros instrumentos da UE, tais como a Diretiva 2011/93/UE relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil (artigo 16.º, n.º 2).

3.5. Direitos fundamentais

A proposta inclui disposições que visam adaptar o quadro jurídico relativo ao combate à fraude e à contrafação de meios de pagamento que não em numerário às ameaças novas e emergentes e regulamentar formas de fraude de meios de pagamento que não em numerário que não se encontram atualmente abrangidas.

O objetivo final destas medidas é proteger os direitos da vítimas e das potenciais vítimas. A criação de um quadro jurídico claro para que as autoridades policiais e judiciais possam atuar diretamente nas atividades criminosas que afetam os dados pessoais das vítimas, incluindo a criminalização dos atos preparatórios, pode ter um impacto particularmente positivo na proteção do direito das vítimas e das potenciais vítimas à privacidade e do direito à proteção dos dados pessoais.

Ao mesmo tempo, todas as medidas previstas na presente proposta respeitam os direitos e liberdades fundamentais consagrados na Carta dos Direitos Fundamentais da União Europeia e devem ser aplicadas em conformidade. Qualquer restrição ao exercício desses direitos e liberdades fundamentais está sujeita às condições enunciadas no artigo 52.º, n.º 1, da Carta, designadamente que têm de observar o princípio da proporcionalidade em relação ao propósito legítimo de corresponder efetivamente a objetivos de interesse geral reconhecidos pela União e proteger os direitos e liberdades de terceiros. As restrições devem estar previstas na lei e respeitar o conteúdo essencial dos direitos e liberdades consagrados na Carta.

Vários direitos e liberdades fundamentais consagrados na Carta foram tidos em conta a este respeito, incluindo: o direito à liberdade e à segurança; o respeito pela vida privada e familiar; a liberdade profissional e o direito a trabalhar; a liberdade de empresa; o direito de propriedade; o direito à ação e a um tribunal imparcial; a presunção de inocência e os direitos de defesa; os princípios da legalidade e da proporcionalidade dos delitos e das penas, bem como o direito a não ser julgado ou punido penalmente mais do que uma vez pelo mesmo delito.

Em particular, a presente proposta respeita o princípio de que as infrações penais e as penas devem estar previstas na lei e ser proporcionadas. Limita o âmbito das infrações ao necessário para permitir uma ação judicial eficaz dos atos que constituem uma ameaça concreta à segurança e introduz regras mínimas em relação ao nível das sanções, em conformidade com o princípio da proporcionalidade, tendo em conta a natureza da infração.

A presente proposta também foi elaborada para assegurar que os dados das pessoas suspeitas das infrações enunciadas na presente diretiva sejam tratados em conformidade com o direito fundamental à proteção dos dados pessoais e com a legislação aplicável existente, incluindo no contexto da cooperação público-privada.

4. INCIDÊNCIA ORÇAMENTAL

A presente proposta não tem incidência imediata no orçamento da UE.

5. OUTROS ELEMENTOS

5.1. Planos de execução e mecanismos de acompanhamento, de avaliação e de informação

A Comissão acompanhará a aplicação da diretiva utilizando as informações apresentadas pelos Estados-Membros sobre as medidas adotadas para pôr em vigor as disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento à diretiva.

Dois anos após o prazo de transposição da presente diretiva, a Comissão deve apresentar um relatório ao Parlamento Europeu e ao Conselho, no qual avalie em que medida os Estados-Membros tomaram as medidas necessárias para dar cumprimento à mesma.

Além disso, a Comissão pretende realizar uma avaliação dos impactos da presente diretiva seis anos após terminar o prazo para a aplicação da mesma, com vista a assegurar que decorre tempo suficiente para avaliar os efeitos da iniciativa após esta ter sido totalmente aplicada em todos os Estados-Membros.

5.2. Documentos explicativos

Não são considerados necessários documentos explicativos sobre a transposição.

6. ELEMENTOS JURÍDICOS DA PROPOSTA

6.1. Síntese da ação proposta

A presente proposta, embora revogue a decisão-quadro 2001/413/JAI, atualiza a maior parte das suas atuais disposições e é coerente com as conclusões da avaliação e da avaliação de impacto (p. ex. no que toca à opção preferida).

O quadro seguinte mostra a correspondência entre a presente proposta e a decisão-quadro e indica quais são os artigos novos e quais são os que foram atualizados em relação à decisão-quadro:

	DIRETIVA		DECISÃO-QUADRO		Observações
	Artigo	**Considerando**	**Artigo**	**Considerando**	
I. Objeto e definições	1. Objeto	1-6	Inexistente	1-7	Novo
	2. Definições	7-8	1. Definições	10	Atualizado
II. Infrações	3. Utilização fraudulenta de instrumentos de pagamento	9	2. Infrações relacionadas com instrumentos de pagamento	8-10	
	4. Infrações preparatórias para a utilização fraudulenta de instrumentos de pagamento				
	5. Infrações relacionadas com sistemas de informação		3. Infrações relacionadas com a informática		
	6. Instrumentos utilizados para cometer infrações		4. Infrações relacionadas com dispositivos especificamente adaptados		
	7. Instigação, auxílio, cumplicidade e tentativa		5. Comparticipação, incitamento e tentativa		
	8. Sanções aplicáveis às pessoas singulares	10-11	6. Sanções	9	
	9. Responsabilidade das pessoas coletivas	Inexistente	7. Responsabilidade das pessoas coletivas	Inexistente	
	10. Sanções aplicáveis a pessoas coletivas		8. Sanções aplicáveis a pessoas coletivas		
III. Competência jurisdicional e investigação	11. Competência jurisdicional	12-14	9. Competência judiciária 10. Extradição e processo penal	11	
	12. Investigações eficazes	15	Inexistente	Inexistente	Novo
IV. Intercâmbio de informações e comunicação de informações sobre crimes	13. Intercâmbio de informações	16-18	11. Cooperação entre os Estados-Membros 12. Intercâmbio de informações	11	Atualizado
	14. Comunicação de informações sobre crimes	19	Inexistente	Inexistente	Novo
V. Assistência e apoio às vítimas e prevenção	15. Assistência e apoio às vítimas	20-22	Inexistente		
	16. Prevenção	23	Inexistente		
VI. Disposições finais	17. Acompanhamento e estatísticas	24	Inexistente		
	18. Substituição da decisão-quadro	25	Inexistente		
	19. Transposição	Inexiste	14. Implementação [artigo 14.º, n.º 1]		Atualizado

	20. Avaliação e relatórios	nte	14. Implementação [artigo 14.º, n.º 2]		
	21. Entrada em vigor		15. Entrada em vigor		
	Inexistente	26-29	13. Âmbito de aplicação territorial		Suprimido

Especificamente, a presente proposta:

- define os instrumentos de pagamento de forma mais abrangente e sólida, incluindo igualmente os instrumentos de pagamento não corpóreos e os meios de troca digitais;

- torna em infração autónoma, para além da utilização destes instrumentos, a posse, venda, obtenção para utilização, importação, distribuição ou disponibilização de um instrumento de pagamento roubado, obtido ilicitamente, contrafeito ou falsificado;

- alarga o âmbito das infrações relacionadas com os sistemas de informação para incluir todas as transações de pagamento, incluindo transações através de meios de troca digitais;

- introduz regras relativas ao nível das penas, definindo em especial um nível mínimo para as penas máximas;

- inclui infrações agravadas em relação a:

- Situações em que os atos criminosos sejam cometidos no âmbito de uma organização criminosa, na aceção da Decisão-Quadro 2008/841/JAI, independentemente da sanção nela prevista;

- situações em que o ato criminoso cause danos agregados consideráveis ou confira um benefício económico considerável aos autores das infrações. Pretende-se assim dar resposta aos casos em que o impacto individual é baixo mas o volume de perdas é grande, especialmente fraudes em que não estão presentes cartões;

- clarifica o âmbito da competência jurisdicional no que diz respeito às infrações referidas na proposta ao assegurar que os Estados-Membros têm competência jurisdicional nos casos em que a infração foi cometida utilizando um sistema de informação localizado no território do Estado-Membro podendo o autor da infração encontrar-se fora desse território ou nos casos em que o autor da infração se encontra dentro do território do Estado-Membro mas o sistema de informação está localizado fora desse território;

- clarifica o âmbito da competência jurisdicional no que diz respeito aos efeitos da infração ao assegurar que os Estados-Membros conseguem exercer a sua competência jurisdicional se a infração causar danos no seu território, incluindo danos resultantes do roubo da identidade de uma pessoa;

- introduz medidas para melhorar a cooperação em matéria de justiça penal em toda a União mediante o reforço da estrutura existente e da utilização dos pontos de contacto operacionais;

- melhora as condições em que as vítimas e as entidades privadas podem comunicar informações sobre crimes;

- satisfaz a necessidade de fornecimento de dados estatísticos sobre fraude e contrafação de meios de pagamento que não em numerário ao obrigar os Estados-Membros a assegurarem a existência de um sistema adequado para registar, produzir e fornecer dados estatísticos sobre as infrações previstas na presente proposta de diretiva;

- prevê que as vítimas tenham acesso a informações sobre os seus direitos e sobre os meios de assistência e apoio disponíveis, independentemente de o seu país de residência ser diferente do país do autor da fraude ou do local onde se estão a efetuar as investigações criminais.

6.2. Explicação pormenorizada das disposições específicas da proposta

Artigo 1.º: Objeto — este artigo define o âmbito e a finalidade da proposta.

Artigo 2.º: Definições — este artigo contém definições aplicáveis a todo o instrumento. O artigo 2.º inclui a mesma definição de moedas virtuais que consta da proposta da Comissão de Diretiva do Parlamento Europeu e do Conselho que altera a Diretiva (UE) 2015/849 relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo e que altera a Diretiva 2009/101/CE[39]. Caso esta definição venha a ser alterada durante o processo de adoção da proposta supramencionada, a definição de moedas virtuais do presente artigo deve ser alinhada em conformidade.

Artigo 3.º: Utilização fraudulenta de instrumentos de pagamento — este artigo enuncia as infrações relacionadas com práticas criminosas que constituem direta e imediatamente fraude, designadamente a utilização fraudulenta de instrumentos de pagamento, incluindo instrumentos roubados e contrafeitos. As infrações são aplicáveis a todos os instrumentos de pagamento, sejam estes corpóreos ou não, pelo que também abrangem as fraudes cometidas com recurso à utilização de credenciais de pagamento ou outros registos roubados ou falsificados que permitam ou sejam utilizados para iniciar uma ordem de pagamento ou outra transferência monetária, incluindo transferências de moeda virtual.

Artigo 4.º: Infrações preparatórias para a utilização fraudulenta de instrumentos de pagamento — este artigo define as infrações relacionadas com práticas criminosas que, embora não constituam imediatamente a verdadeira fraude que conduz à perda de bens, são cometidas para preparar a fraude. Estão incluídos o furto ou a contrafação de um instrumento de pagamento e vários atos envolvidos no tráfico desses instrumentos roubados ou contrafeitos. Inclui a posse, distribuição ou disponibilização com vista à sua utilização fraudulenta, incluindo casos em que o autor da infração está ciente da possibilidade de utilização fraudulenta (*dolus eventualis*). Tal como acontece no artigo 3.º, abrange todas as infrações que envolvam instrumentos de pagamento, sejam estes corpóreos ou não, e, por conseguinte, também é aplicável a comportamentos como a comercialização de credenciais roubadas («*carding*») e *phishing*[40].

---

39 COM(2016) 450 final.

40 *Phishing* é um método utilizado pelos autores das fraudes para aceder a informações pessoais valiosas, tais como nomes de utilizador e palavras-passe. A forma mais comum de *phishing* é o envio de um e-mail que aparentemente provém de uma empresa conhecida e de confiança para uma grande lista de endereços eletrónicos. O e-mail pode direcionar o recipiente para uma página Web falsa, onde é pedido que a pessoa visada forneça informações pessoais.

Artigo 5.º: Infrações relacionadas com sistemas de informação — este artigo define as infrações relacionadas com sistemas de informação, que devem ser criminalizadas pelos Estados-Membros. A lista contém elementos que distinguem as infrações da interferência ilegal em sistemas ou da interferência ilegal nos dados que constam da Diretiva 2013/40/UE, tais como a transferência de valores monetários para obter um ganho ilícito. Esta disposição foi incluída com vista a criminalizar práticas como o acesso ilegal ao computador ou dispositivo da vítima («*hacking*») para redirecionar o tráfego da vítima para um sítio bancário falso em linha, levando assim a vítima a efetuar um pagamento para uma conta bancária controlada pelo autor da infração («internautas que lavam dinheiro»)[41]. Abrange igualmente outras formas de prática criminosa como o *pharming*[42], que explora os sistemas de informação para conseguir um ganho ilícito para o autor da infração ou outra pessoa.

Artigo 6.º: Instrumentos utilizados para cometer infrações — este artigo define as infrações relacionadas com os instrumentos utilizados para cometer as infrações previstas no artigo 4.º, alíneas a) e b), e no artigo 5.º, que devem ser criminalizadas pelos Estados-Membros. Tem como objetivo criminalizar a produção, a venda, a obtenção para utilização, a importação, a distribuição ou a disponibilização intencionais de, por exemplo, dispositivos de *skimming* utilizados para roubar credenciais, bem como *malware* e sítios web falsos utilizados para *phishing*. Este artigo baseia-se em grande medida no artigo 4.º da Decisão-Quadro 2001/413/JAI e no artigo 3.º, alínea d), subalínea i), da Diretiva 2014/62/UE relativa à proteção penal do euro e de outras moedas contra a contrafação.

Artigo 7.º: Instigação, auxílio, cumplicidade e tentativa — este artigo é aplicável a práticas relacionadas com as infrações previstas nos artigos 3.º a 6.º e exige a criminalização pelos Estados-Membros de todas as formas de preparação e participação. A responsabilidade penal por tentativa está incluída nas infrações previstas nos artigos 3.º a 6.º.

Artigo 8.º: Sanções para pessoas singulares — para combater eficazmente a fraude e a contrafação de meios de pagamento que não em numerário, as sanções devem ser dissuasoras em todos os Estados-Membros. Em consonância com outros instrumentos da UE que aproximam o nível das sanções penais, este artigo estipula que a pena máxima ao abrigo do direito nacional deve ser, no mínimo, de três anos de prisão, com exceção das infrações que constam do artigo 6.º, em relação às quais as penas máximas devem ser, no mínimo, de dois anos. Prevê sanções mais graves para as infrações agravadas, designadamente uma pena máxima de, no mínimo, cinco anos, quando o crime é cometido por uma organização criminosa, na aceção da Decisão-Quadro 2008/841/JAI do Conselho, de 24 de outubro de 2008, relativa à luta contra a criminalidade organizada[43], ou quando um crime é cometido em grande escala, causando assim danos alargados ou consideráveis, incluindo em especial casos com impacto individual reduzido mas com efeitos globais de grande dimensão, ou quando um crime envolve uma vantagem agregada para o autor da infração de, pelo menos, 20 000 EUR.

---

41 O termo «agir na qualidade de internauta que lava dinheiro» indica uma pessoa que transfere produtos do crime entre diferentes países. Os internautas que lavam dinheiro recebem os produtos do crime nas suas contas, sendo-lhes então pedido que levantem o dinheiro e o transfiram para uma conta diferente, frequentemente no estrangeiro, ficando com algum do dinheiro para si (ActionFraudUK, 2017). Por vezes, sabem que os fundos advêm da atividade criminosa; outras vezes, são levados a acreditar que os fundos são genuínos.

42 *Pharming* é uma prática utilizada para enganar as pessoas mediante a qual se instala um código malicioso num computador pessoal ou num servidor, direcionando enganadoramente os utilizadores para sítios web fraudulentos sem o seu conhecimento ou consentimento.

43 JO L 300 de 11.11.2008, p. 42.

As infrações enunciadas nos artigos 2.º a 5.º da Decisão-Quadro 2001/413/JAI parecem ser puníveis com sanções específicas na maioria dos Estados-Membros que têm informações disponíveis. Contudo, em geral, não existe aproximação: ainda que todos os Estados-Membros tenham sanções que implicam privação de liberdade (pelo menos, em casos graves), verifica-se que o nível das sanções para a mesma prática varia significativamente. Consequentemente, o efeito dissuasor é mais reduzido nalguns Estados-Membros do que noutros.

As disparidades no nível das sanções pode também impedir a cooperação judicial. Se o código penal de um Estado-Membro prevê penas mínimas baixas, este facto pode implicar a atribuição por parte das autoridades policiais e judiciais de um baixo nível de prioridade à investigação e repressão de fraudes em que não estão presentes cartões. Trata-se de algo que, por seu turno, pode impedir a cooperação transfronteiriça quando outro Estado-Membro solicita assistência, em termos do tratamento atempado de um pedido. Provavelmente, quem mais beneficiará dessas disparidades serão os autores das infrações mais graves, ou seja, grupos da criminalidade organizada transnacionais com bases de operações em vários Estados-Membros.

Artigos 9.º e 10.º: Responsabilidade e sanções para pessoas coletivas — estes artigos são aplicáveis a todas as infrações previstas nos artigos 3.º a 7.º. É exigido aos Estados-Membros que assegurem a responsabilidade das pessoas coletivas, sem excluir a responsabilidade das pessoas singulares, e apliquem sanções efetivas, proporcionadas e dissuasoras às pessoas coletivas. O artigo 10.º dá exemplos de sanções.

Artigo 11.º: Competência jurisdicional — com base nos princípios da territorialidade e da personalidade, este artigo enuncia as situações em que os Estados-Membros devem estabelecer a sua jurisdição para as infrações previstas nos artigos 3.º a 7.º.

Inclui elementos retirados do artigo 12.º da Diretiva 2013/40/UE relativa a ataques contra os sistemas de informação. Nos casos em que a fraude e a contrafação de meios de pagamento que não em numerário ocorram em linha, é provável que o crime abranja várias jurisdições: é frequentemente cometido utilizando sistemas de informação fora do território em que o autor da infração se encontra fisicamente e tem consequências noutro país onde as provas também podem estar localizadas. Por conseguinte, o artigo 11.º pretende assegurar que a jurisdição territorial abrange situações em que o autor da infração e o sistema de informação utilizado pelo autor da infração para cometer o crime se encontram em territórios diferentes.

Este artigo inclui um novo elemento que dá resposta à necessidade de declarar a competência jurisdicional se o dano for causado numa jurisdição diferente daquela em que a prática ocorreu, incluindo danos resultantes do roubo de identidade de uma pessoa. O objetivo é abranger situações não previstas na Diretiva 2013/40/UE relativa a ataques contra os sistemas de informação, que são comuns aos crimes de fraude de meios de pagamento que não em numerário. Incluem-se casos como aqueles em que nenhuma das infrações associadas ao crime (p. ex. roubo de credenciais de cartões, clonagem de um cartão, levantamento ilegal de uma caixa multibanco) foi cometida no Estado-Membro em que os danos ocorreram (p. ex. onde a vítima tem a conta bancária da qual foi roubado o dinheiro). Nestes casos, é provável que a vítima comunique o incidente às autoridades do Estado-Membro em que as perdas económicas foram detetadas. É necessário que esse Estado-Membro seja capaz de exercer jurisdição para assegurar a eficácia da investigação e da ação judicial, servindo de ponto de partida para as investigações que podem envolver múltiplos Estados-Membros e países fora da UE.

Artigo 12.º: Investigações eficazes — este artigo tem como objetivo assegurar que os instrumentos de investigação previstos no direito nacional para a criminalidade organizada ou outros crimes graves também podem ser utilizados nos casos de fraude e contrafação de meios de pagamento que não em numerário, pelo menos nos casos mais graves. Este artigo pretende também assegurar que, no seguimento de injunções legais, o fornecimento das informações às autoridades acontece sem atrasos indevidos.

Artigo 13.º: Intercâmbio de informações — este artigo tem como objetivo incentivar uma maior utilização dos pontos de contacto operacionais nacionais.

Artigo 14.º: Comunicação de informações sobre crimes — este artigo tem como objetivo dar resposta à necessidade identificada na avaliação de impacto de aumentar e facilitar a comunicação de informações. Procura assegurar a disponibilidade de canais adequados que as vítimas e as entidades privadas possam utilizar para comunicar informações sobre crimes, bem como incentivar a comunicação de informações sem atrasos indevidos em consonância com uma disposição idêntica que consta do artigo 16.º, n.º 2, da Diretiva 2011/93/UE relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil. No considerando 19 é possível encontrar exemplos de ações a realizar.

Artigo 15.º: Assistência e apoio às vítimas — este artigo exige que os Estados-Membros assegurem que as vítimas de fraude de meios de pagamento que não em numerário tenham à sua disposição informações e canais para comunicar um crime, bem como aconselhamento sobre como se podem proteger contra as consequências negativas da fraude e contra os danos reputacionais daí decorrentes.

Este artigo abrange tanto as pessoas singulares como as pessoas coletivas, que também são afetadas pelas consequências das infrações que constam da presente proposta. Introduz igualmente disposições que visam alargar às pessoas coletivas diversos direitos específicos estabelecidos para as pessoas singulares na Diretiva 2012/29/UE.

Artigo 16.º: Prevenção — este artigo dá resposta à necessidade de uma maior sensibilização, reduzindo assim o risco de alguém se tornar vítima de fraude, através de campanhas de informação e sensibilização e de programas de investigação e educação. A avaliação de impacto identificou as lacunas na prevenção como um dos principais problemas subjacentes à fraude de meios de pagamento que não em numerário. Este artigo segue uma abordagem idêntica à do artigo 23.º (Prevenção) da Diretiva 2011/93/UE relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil.

Artigo 17.º: Acompanhamento e estatísticas — este artigo satisfaz a necessidade de fornecimento de dados estatísticos sobre fraude e contrafação de meios de pagamento que não em numerário ao torná-lo obrigatório para os Estados-Membros, com vista a assegurar que existe um sistema adequado de registo, produção e fornecimento de dados estatísticos sobre as infrações previstas na presente proposta de diretiva e sobre o acompanhamento da eficácia dos seus sistemas (abrangendo todas as fases judiciais) de combate à fraude de meios de pagamento que não em numerário. Segue uma abordagem idêntica à do artigo 14.º (Acompanhamento e estatísticas) da Diretiva 2013/40/UE relativa a ataques contra os sistemas de informação e à do artigo 44.º da Diretiva (UE) 2015/849 relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo (quarta Diretiva Antibranqueamento de Capitais). Pretende também contribuir para dar resposta à disponibilidade limitada de dados sobre fraude que

atualmente existe, algo que pode ajudar a avaliar a eficácia dos sistemas nacionais de combate à fraude de meios de pagamento que não em numerário.

Artigo 18.º: Substituição da Decisão-Quadro 2001/413/JAI — este artigo substitui as atuais disposições no domínio da fraude e da contrafação de meios de pagamento que não em numerário destinadas aos Estados-Membros que participam na presente diretiva.

Artigos 19.º, 20.º e 21.º — estes artigos contêm disposições sobre transposição pelos Estados-Membros, avaliação e apresentação de relatórios pela Comissão e entrada em vigor da diretiva.

2017/0226 (COD)

Proposta de

DIRETIVA DO PARLAMENTO EUROPEU E DO CONSELHO

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

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 83.º, n.º 1,

Tendo em conta a proposta da Comissão Europeia,

Após transmissão do projeto de ato legislativo aos parlamentos nacionais,

Tendo em conta o parecer do Comité Económico e Social Europeu,

Deliberando de acordo com o processo legislativo ordinário,

Considerando o seguinte:

(1) A fraude e a contrafação de meios de pagamento que não em numerário constituem uma ameaça à segurança, uma vez que representam uma fonte de rendimento para a criminalidade organizada, sendo, por conseguinte, uma forma de facilitar outras atividades criminosas como o terrorismo, o tráfico de estupefacientes e o tráfico de seres humanos.

(2) A fraude e a contrafação de meios de pagamento que não em numerário constituem também um obstáculo ao mercado único digital, uma vez que afetam negativamente a confiança dos consumidores e provocam perdas económicas diretas.

(3) A Decisão-Quadro 2001/413/JAI do Conselho[44] necessita de ser atualizada e complementada com mais algumas disposições sobre infrações, sanções e cooperação transfronteiriça.

(4) A existência de lacunas e de diferenças significativas no direito dos Estados-Membros no domínio da fraude e da contrafação de meios de pagamento que não em numerário pode dificultar a luta contra este tipo de criminalidade e contra outros crimes graves e organizados relacionados ou derivados desta, podendo igualmente complicar a eficácia da cooperação policial e judiciária neste domínio.

[44] Decisão-Quadro 2001/413/JAI do Conselho, de 28 de maio de 2001, relativa ao combate à fraude e à falsificação de meios de pagamento que não em numerário (JO L 149 de 2.6.2001, p. 1).

(5) A fraude e a contrafação de meios de pagamento que não em numerário têm uma dimensão transfronteiriça significativa, acentuada pela componente digital, que realça a necessidade de mais ação para aproximar a legislação penal neste domínio.

(6) Nos últimos anos, assistiu-se não apenas a um aumento exponencial da economia digital, mas também à proliferação da inovação em muitos domínios, incluindo nas tecnologias de pagamento. As novas tecnologias de pagamento implicam a utilização de novos tipos de instrumentos de pagamento, que, apesar de criarem novas oportunidades para consumidores e empresas, também aumentam as oportunidades de fraude. Consequentemente, o quadro jurídico deve permanecer pertinente e atualizado em relação a estes avanços tecnológicos.

(7) É importante adotar definições comuns neste domínio para assegurar uma abordagem coerente na aplicação da presente diretiva nos Estados-Membros. Importa que as definições abranjam novos tipos de instrumentos de pagamento, tais como o dinheiro eletrónico e as moedas virtuais.

(8) Ao conferir-se proteção, através do direito penal, sobretudo aos instrumentos de pagamento dotados de uma forma especial de proteção contra imitações ou utilização abusiva, pretende-se incentivar os operadores a proporcionar essas formas especiais de proteção aos instrumentos de pagamento que emitem, acrescentando-lhes assim um elemento de prevenção.

(9) A existência de medidas eficazes e eficientes no direito penal é fundamental para proteger os meios de pagamento que não em numerário contra a fraude e a contrafação. É especialmente necessária uma abordagem penal comum no que toca aos elementos constituintes de prática criminosa que possam contribuir ou preparar o terreno para a efetiva utilização fraudulenta dos meios de pagamento. Comportamentos como a recolha e a posse de instrumentos de pagamento com intenção de cometer uma fraude através, por exemplo, de *phishing* (acesso fraudulento a informações pessoais) ou *skimming* (cópia dos dados de um cartão) e respetiva distribuição (por exemplo, vender informações sobre cartões de crédito na Internet) devem portanto constituir uma infração penal por direito próprio sem estarem diretamente ligados à efetiva utilização fraudulenta dos meios de pagamento. Assim sendo, tal prática criminosa deve igualmente abranger circunstâncias em que a posse, a aquisição ou a distribuição não conduzam necessariamente à utilização fraudulenta desses instrumentos de pagamento, se o autor da infração estiver consciente dessa possibilidade (*dolus eventualis*). A presente diretiva não sanciona a utilização legítima de um instrumento de pagamento, incluindo e em relação à prestação de serviços de pagamento inovadores, tais como os serviços habitualmente desenvolvidos pelas empresas ligadas às tecnologias financeiras.

(10) As sanções e penas aplicáveis à fraude e à contrafação de meios de pagamento que não em numerário devem ser efetivas, proporcionadas e dissuasoras em toda a União.

(11) Considera-se adequado prever sanções mais graves quando o crime é cometido por uma organização criminosa, na aceção da Decisão-Quadro 2008/841/JAI do Conselho[45], ou quando um crime é cometido em grande escala, causando danos

[45] Decisão-Quadro 2008/841/JAI do Conselho, de 24 de outubro de 2008, relativa à luta contra a criminalidade organizada (JO L 300 de 11.11.2008, p. 42).

alargados ou consideráveis às vítimas ou envolvendo uma vantagem agregada para o autor da infração, no mínimo, de 20 000 EUR.

(12) As regras relativas à competência jurisdicional devem assegurar a eficácia da ação penal em relação às infrações previstas na presente diretiva. Em geral, o sistema penal do país em que as infrações são cometidas é o mais adequado para as sancionar. Por conseguinte, os Estados-Membros devem estabelecer a respetiva competência jurisdicional em relação a infrações cometidas nos seus territórios, a infrações cometidas pelos seus cidadãos nacionais e a infrações que causam danos nos seus territórios.

(13) Os sistemas de informação desafiam o conceito tradicional de territorialidade, uma vez que, em princípio, podem ser utilizados e controlados remotamente a partir de qualquer lugar. Sempre que os Estados-Membros declarem a competência jurisdicional com base nas infrações cometidas nos seus territórios, parece adequado avaliar também o âmbito da sua competência nos casos em que as infrações são cometidas com recurso a sistemas de informação. Nestes casos, a competência jurisdicional deve abranger situações em que o sistema de informação esteja localizado no território do Estado-Membro ainda que o autor da infração possa encontrar-se fora do território, bem como situações em que o autor da infração esteja localizado no território do Estado-Membro ainda que o sistema de informação possa estar localizado fora deste.

(14) Importa abordar a complexidade da atribuição da competência jurisdicional no que diz respeito aos efeitos da infração numa jurisdição diferente daquela em que ocorreu o ato propriamente dito. Assim, a competência jurisdicional deve ser declarada para infrações cometidas pelos autores das infrações independentemente da nacionalidade e presença física dos mesmos, mas considerando quaisquer danos causados por um ato desses no território do Estado-Membro.

(15) Dada a necessidade de instrumentos especiais para investigar eficazmente a fraude e a contrafação de meios de pagamento que não em numerário, bem como a sua pertinência para uma cooperação internacional eficaz entre autoridades nacionais, importa disponibilizar instrumentos de investigação tipicamente utilizados em casos que envolvem criminalidade organizada e outro tipo de criminalidade grave às autoridades competentes em todos os Estados-Membros para a investigação dessas infrações penais. Tendo em conta, o princípio da proporcionalidade, a utilização desses instrumentos em conformidade com o direito nacional deverá ser adaptada à natureza e à gravidade das infrações penais investigadas. Além disso, as autoridades policiais e outras autoridades competentes devem poder aceder atempadamente a informações pertinentes por forma a investigarem e reprimirem as infrações previstas na presente diretiva.

(16) Em muitos casos, as atividades criminosas estão na base de incidentes que devem ser notificados às autoridades nacionais competentes pertinentes ao abrigo da Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho[46]. Tais incidentes podem levantar suspeitas quanto à sua natureza criminosa mesmo que os indícios de uma

[46] Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (JO L 194 de 19.7.2016, p. 1).

infração penal não sejam suficientemente claros desde o início. Neste contexto, os operadores de serviços essenciais pertinentes e os prestadores de serviços digitais devem ser incentivados a partilhar os relatórios exigidos ao abrigo da Diretiva (UE) 2016/1148 com as autoridades policiais por forma a dar uma resposta eficaz e abrangente e a facilitar a imputação e a responsabilização dos autores das infrações pelas suas ações. Em especial, a promoção de um ambiente seguro, protegido e mais resiliente requer a notificação sistemática dos incidentes que se suspeite terem uma origem criminosa grave às autoridades responsáveis. Além disso, quando for pertinente, importa que as equipas de resposta a incidentes de segurança informática previstas no artigo 9.º da Diretiva (UE) 2016/1148 sejam envolvidas nas investigações policiais com vista a fornecerem informações, consoante for considerado adequado a nível nacional, e também a transmitirem conhecimentos especializados sobre sistemas de informação.

(17) Os incidentes de segurança de caráter severo tal como definidos no artigo 96.º da Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho[47] podem ter origem criminosa. Sempre que pertinente, os prestadores de serviços de pagamento devem ser incentivados a partilhar com as autoridades policiais os relatórios que são obrigados a apresentar à autoridade competente no respetivo Estado-Membro de acolhimento ao abrigo da Diretiva (UE) 2015/2366.

(18) Existem vários instrumentos e mecanismos ao nível da União que permitem o intercâmbio de informações entre as autoridades policiais nacionais para fins de investigação e repressão da criminalidade. Para facilitar e acelerar a cooperação entre as autoridades policiais nacionais e garantir que estes instrumentos e mecanismos são utilizados em pleno, a presente diretiva deve reforçar a importância dos pontos de contacto operacionais introduzidos pela Decisão-Quadro 2001/413/JAI do Conselho. Os Estados-Membros podem decidir utilizar a rede de pontos de contacto operacionais já existente, como a que foi estabelecida na Diretiva 2013/40/UE do Parlamento Europeu e do Conselho[48]. Cabe-lhes prestar assistência de forma eficaz, por exemplo, facilitando o intercâmbio de informações pertinentes e a disponibilização de aconselhamento técnico ou informações jurídicas. Para assegurar o bom funcionamento da rede, cada ponto de contacto deve conseguir comunicar rapidamente com o ponto de contacto de outro Estado-Membro. Tendo em conta a significativa dimensão transfronteiriça deste domínio da criminalidade e, em particular, a natureza volátil das provas eletrónicas, os Estados-Membros devem ser capazes de dar prontamente resposta aos pedidos urgentes desta rede de pontos de contacto e fornecer informações no prazo de oito horas.

(19) Comunicar informações sobre crimes sem atrasos indevidos às autoridades públicas é extremamente importante no combate à fraude e à contrafação de meios de pagamento que não em numerário, uma vez que essas informações são muitas vezes o ponto de partida da investigação penal. Importa tomar medidas para incentivar a comunicação

---

47 Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, relativa aos serviços de pagamento no mercado interno, que altera as Diretivas 2002/65/CE, 2009/110/CE e 2013/36/UE e o Regulamento (UE) n.º 1093/2010, e que revoga a Diretiva 2007/64/CE (JO L 337 de 23.12.2015, p. 35).

48 Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho (JO L 218 de 14.8.2013, p. 8).

de informações por parte de pessoas singulares e pessoas coletivas, em especial instituições financeiras, às autoridades policiais e judiciárias. Estas medidas podem basear-se em vários tipos de ações, nomeadamente ações legislativas, tais como obrigações de comunicação de suspeitas de fraude, ou ações não legislativas, tais como criar ou apoiar organizações ou mecanismos que favoreçam o intercâmbio de informações, ou sensibilização. Qualquer medida que envolva o tratamento de dados pessoais de pessoas singulares deve ser tomada em conformidade com o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho[49]. Em especial, qualquer transmissão de informações relativa à prevenção e ao combate de infrações relacionadas com a fraude e a contrafação de meios de pagamento que não em numerário deve cumprir os requisitos definidos no Regulamento (UE) 2016/679, designadamente os fundamentos jurídicos do tratamento.

(20) A fraude e a contrafação de meios de pagamento que não em numerário pode ter consequências económicas e não económicas graves para as vítimas. Quando a fraude envolve o roubo da identidade, as consequências são ainda mais gravosas devido aos graves danos emocionais e reputacionais que acarreta. Os Estados-Membros devem adotar medidas de assistência, apoio e proteção destinadas a atenuar estas consequências.

(21) As pessoas singulares que sejam vítimas de fraude relacionada com meios de pagamento que não em numerário têm direitos que lhes foram conferidos pela Diretiva 2012/29/UE do Parlamento Europeu e do Conselho[50]. Os Estados-Membros devem adotar medidas de assistência e apoio às referidas vítimas que assentem nas medidas previstas na Diretiva 2012/29/UE mas que satisfaçam mais diretamente as necessidades específicas das vítimas de fraude relacionada com o roubo de identidade. Estas medidas devem incluir, mais concretamente, apoio psicológico especializado e aconselhamento sobre questões financeiras, práticas e jurídicas, bem como assistência no que toca a receber eventuais indemnizações. Também devem ser disponibilizadas informações específicas e aconselhamento sobre proteção contra as consequências negativas deste tipo de criminalidade às pessoas coletivas.

(22) A presente diretiva deve prever o direito que assiste às pessoas coletivas de aceder a informações acerca dos procedimentos para apresentar denúncias. Este direito é especialmente necessário para as pequenas e médias empresas[51] e deve contribuir para criar um ambiente empresarial mais favorável para as pequenas e médias empresas. As pessoas singulares já beneficiam deste direito nos termos da Diretiva 2012/29/UE.

(23) Os Estados-Membros devem estabelecer ou reforçar políticas para prevenir a fraude e a contrafação de meios de pagamento que não em numerário, bem como medidas para reduzir o risco de se tornarem vítimas dessas infrações, através de campanhas de informação e sensibilização e programas de investigação e educação.

---

49 Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral da Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

50 Diretiva 2012/29/UE do Parlamento Europeu e do Conselho, de 25 de outubro de 2012, que estabelece normas mínimas relativas aos direitos, ao apoio e à proteção das vítimas da criminalidade e que substitui a Decisão-Quadro 2001/220/JAI do Conselho (JO L 315 de 14.11.2012, p. 57).

51 Recomendação da Comissão de 6 de maio de 2003 relativa à definição de micro, pequenas e médias empresas (JO L 124 de 20.5.2003, p. 36).

(24) É necessário recolher dados comparáveis sobre as infrações penais previstas na presente diretiva. Importa disponibilizar dados pertinentes às agências e organismos da União competentes e especializados, em particular à Europol, em consonância com as suas funções e necessidades de informação. O objetivo é conseguir-se uma visão mais completa do problema da fraude e da contrafação de meios de pagamento que não em numerário e das questões relacionadas com a segurança dos pagamentos ao nível da União e, dessa forma, contribuir para formular uma resposta mais eficaz. Os Estados-Membros devem tirar o máximo partido do mandato da Europol e da sua capacidade de dar assistência e apoiar as investigações pertinentes, fornecendo informações sobre o *modus operandi* dos autores das infrações à Europol com vista à realização de análises estratégicas e avaliações de ameaças em matéria de fraude e contrafação de meios de pagamento que não em numerário em conformidade com o Regulamento (UE) 2016/794 do Parlamento Europeu e do Conselho[52]. O fornecimento de informações pode contribuir para uma melhor compreensão das ameaças presentes e futuras e ajudar o Conselho e a Comissão a definirem as prioridades estratégicas e operacionais da União em matéria de luta contra a criminalidade e as formas de aplicar essas prioridades.

(25) A presente diretiva visa alterar e alargar as disposições da Decisão-Quadro 2001/413/JAI do Conselho. Dado que as alterações a introduzir são substanciais tanto em número como em natureza, a Decisão-Quadro 2001/413/JAI deverá, por uma questão de clareza, ser integralmente substituída no que se refere aos Estados-Membros que se encontram vinculados pela presente diretiva.

(26) Nos termos do artigo 3.º do Protocolo n.º 21 relativo à posição do Reino Unido e da Irlanda em relação ao espaço de liberdade, segurança e justiça, anexo ao Tratado da União Europeia e ao Tratado sobre o Funcionamento da União Europeia, estes Estados-Membros notificaram por escrito a sua intenção de participar na adoção e aplicação da presente diretiva.

OU

(26) Nos termos do artigo 3.º do Protocolo n.º 21 relativo à posição do Reino Unido e da Irlanda em relação ao espaço de liberdade, segurança e justiça, anexo ao Tratado da União Europeia e ao Tratado sobre o Funcionamento da União Europeia, o Reino Unido notificou [, por carta de ...,] a intenção de participar na adoção e na aplicação da presente diretiva.

OU

(26) Nos termos do artigo 3.º do Protocolo n.º 21 relativo à posição do Reino Unido e da Irlanda em relação ao espaço de liberdade, segurança e justiça, anexo ao Tratado da União Europeia e ao Tratado sobre o Funcionamento da União Europeia, a Irlanda notificou [, por carta de ...,] a intenção de participar na adoção e aplicação da presente diretiva.

---

52 Regulamento (UE) 2016/794 do Parlamento Europeu e do Conselho, de 11 de maio de 2016, que cria a Agência da União Europeia para a Cooperação Policial (Europol) e que substitui e revoga as Decisões 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI e 2009/968/JAI do Conselho (JO L 135 de 24.5.2016, p. 53).

E/OU

(26) Em conformidade com os artigos 1.º e 2.º do Protocolo n.º 21 relativo à posição do Reino Unido e da Irlanda em relação ao espaço de liberdade, segurança e justiça, anexo ao Tratado da União Europeia e ao Tratado sobre o Funcionamento da União Europeia, e sem prejuízo do seu artigo 4.º, estes Estados-Membros não participam na adoção nem na aplicação da presente diretiva, não ficando por ela vinculados nem sujeitos à sua aplicação.

OU

(26) Em conformidade com os artigos 1.º e 2.º do Protocolo n.º 21 relativo à posição do Reino Unido e da Irlanda em relação ao espaço de liberdade, segurança e justiça, anexo ao Tratado da União Europeia e ao Tratado sobre o Funcionamento da União Europeia, e sem prejuízo do seu artigo 4.º, a Irlanda não participa na adoção nem na aplicação da presente diretiva, não ficando por ela vinculada nem sujeita à sua aplicação.

OU

(26) Em conformidade com os artigos 1.º e 2.º do Protocolo n.º 21 relativo à posição do Reino Unido e da Irlanda em relação ao espaço de liberdade, segurança e justiça, anexo ao Tratado da União Europeia e ao Tratado sobre o Funcionamento da União Europeia, e sem prejuízo do seu artigo 4.º, o Reino Unido não participa na adoção nem na aplicação da presente diretiva, não ficando por ela vinculado nem sujeito à sua aplicação.

(27) Nos termos dos artigos 1.º e 2.º do Protocolo n.º 22 relativo à posição da Dinamarca, anexo ao Tratado da União Europeia e ao Tratado sobre o Funcionamento da União Europeia, a Dinamarca não participa na adoção da presente diretiva e não fica a ela vinculada nem sujeita à sua aplicação.

(28) Atendendo a que os objetivos da presente diretiva, a saber, sujeitar a fraude e a contrafação de meios de pagamento que não em numerário a sanções penais efetivas, proporcionadas e dissuasoras e melhorar e incentivar a cooperação transfronteiriça tanto entre as autoridades competentes como entre as pessoas singulares e coletivas e as autoridades competentes, não podem ser suficientemente alcançados pelos Estados-Membros, mas podem, devido à sua dimensão ou aos seus efeitos, ser mais bem alcançados ao nível da União, a União pode tomar medidas em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do Tratado da União Europeia. Em conformidade com o princípio da proporcionalidade consagrado no mesmo artigo, a presente diretiva não excede o necessário para alcançar esses objetivos.

(29) A presente diretiva respeita os direitos fundamentais e observa os princípios reconhecidos, nomeadamente, na Carta dos Direitos Fundamentais da União Europeia, incluindo o direito à liberdade e à segurança, o direito ao respeito pela vida privada e familiar, a proteção dos dados pessoais, a liberdade de empresa, o direito de propriedade, o direito à ação e a um tribunal imparcial, a presunção de inocência e o direito de defesa, os princípios da legalidade e da proporcionalidade dos delitos e das penas, bem como o direito a não ser julgado ou punido penalmente mais do que uma vez pelo mesmo delito. A presente diretiva procura assegurar o pleno respeito desses direitos e princípios e deverá ser aplicada em conformidade,

ADOTARAM A PRESENTE DIRETIVA:

TÍTULO I: OBJETO E DEFINIÇÕES

Artigo 1.º
Objeto

A presente diretiva estabelece regras mínimas relativas à definição das infrações penais e das sanções no domínio da fraude e da contrafação de meios de pagamento que não em numerário.

Artigo 2.º
Definições

Para efeitos da presente diretiva, entende-se por:

(a) «Instrumento de pagamento», um dispositivo, objeto ou registo protegido, diferente da moeda em curso legal, que, por si só ou com um procedimento ou um conjunto de procedimentos, permite ao titular ou utilizador transferir dinheiro ou valor monetário ou iniciar uma ordem de pagamento, incluindo através de meios de troca digitais;

(b) «Dispositivo, objeto ou registo protegido», um dispositivo, objeto ou registo salvaguardado contra imitação ou utilização fraudulenta, por exemplo, através da sua conceção, codificação ou assinatura;

(c) «Ordem de pagamento», uma ordem de pagamento na aceção do artigo 4.º, ponto 13, da Diretiva (UE) 2015/2366;

(d) «Meio de troca digital», qualquer tipo de moeda eletrónica na aceção do artigo 2.º, ponto 2, da Diretiva 2009/110/CE do Parlamento Europeu e do Conselho[53], e moedas virtuais;

(e) «Moeda virtual», uma representação digital de valor que não tenha sido emitida por um banco central ou uma autoridade pública, nem esteja necessariamente ligada a uma moeda fiduciária, mas que é aceite por pessoas singulares ou coletivas como meio de pagamento e possa ser transferida, armazenada ou comercializada por via eletrónica;

(f) «Serviço de pagamento», um serviço de pagamento na aceção do artigo 4.º, ponto 3, da Diretiva (UE) 2015/2366;

(g) «Utilizador de serviços de pagamento», um utilizador de serviços de pagamento na aceção do artigo 4.º, ponto 10, da Diretiva (UE) 2015/2366;

[53] 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, p. 7).

(h) «Conta de pagamento», uma conta de pagamento na aceção do artigo 4.º, ponto 12, da Diretiva (UE) 2015/2366;

(i) «Operação de pagamento», uma operação de pagamento na aceção do artigo 4.º, ponto 5, da Diretiva (UE) 2015/2366;

(j) «Ordenante», uma pessoa singular ou coletiva que detém uma conta de pagamento e que autoriza uma ordem de pagamento a partir dessa conta ou, caso não exista conta de pagamento, uma pessoa singular ou coletiva que emite uma ordem de pagamento ou transfere moeda virtual;

(k) «Beneficiário», um beneficiário na aceção do artigo 4.º, ponto 9, da Diretiva (UE) 2015/2366;

(l) «Sistema de informação», um sistema de informação na aceção do artigo 2.º, alínea a), da Diretiva 2013/40/UE;

(m) «Dados informáticos», dados informáticos na aceção do artigo 2.º, alínea b), da Diretiva 2013/40/UE.

TÍTULO II: INFRAÇÕES

Artigo 3.º
Utilização fraudulenta de instrumentos de pagamento

Os Estados-Membros devem tomar as medidas necessárias para assegurar que, quando cometidos com dolo, os seguintes atos sejam puníveis como infrações penais:

(a) A utilização fraudulenta de um instrumento de pagamento roubado ou obtido ilicitamente;

(b) A utilização fraudulenta de um instrumento de pagamento contrafeito ou falsificado.

Artigo 4.º
Infrações preparatórias para a utilização fraudulenta de instrumentos de pagamento

Os Estados-Membros devem tomar as medidas necessárias para assegurar que, quando cometidos com dolo, os seguintes atos sejam puníveis como infrações penais:

(a) O furto ou outra forma de apropriação ilícita de instrumentos de pagamento;

(b) A contrafação ou falsificação de um instrumento de pagamento, a fim de ser utilizado fraudulentamente;

(c) A posse, obtenção para utilização, importação, exportação, venda, transporte, distribuição ou disponibilização de um instrumento de pagamento roubado, obtido ilicitamente, contrafeito ou falsificado com vista a ser utilizado fraudulentamente.

Artigo 5.º
Infrações relacionadas com sistemas de informação

Os Estados-Membros devem tomar as medidas necessárias para assegurar que, quando cometidos com dolo, sejam punidos como infrações penais os atos de efetuar ou levar à realização de uma transferência de dinheiro, valor monetário ou moedas virtuais, com vista a que o autor da infração ou outra pessoa obtenha um ganho ilícito, que impliquem:

(a) Manipular ou interferir com o funcionamento de um sistema de informação;

(b) Introduzir, alterar, eliminar, transmitir ou suprimir dados informáticos.

Artigo 6.º
Instrumentos utilizados para cometer infrações

Os Estados-Membros devem tomar as medidas necessárias para assegurar que, quando cometidos com intenção fraudulenta, sejam puníveis como infrações penais a produção, obtenção para utilização, importação, exportação, venda, transporte, distribuição ou disponibilização de um dispositivo ou instrumento, dados informáticos ou quaisquer outros meios especificamente concebidos ou adaptados com o intuito de cometer qualquer uma das infrações previstas no artigo 4.º, alíneas a) e b), ou no artigo 5.º.

Artigo 7.º
Instigação, auxílio, cumplicidade e tentativa

1. Os Estados-Membros devem tomar as medidas necessárias para que a instigação, o auxílio ou a cumplicidade para cometer uma infração prevista nos artigos 3.º a 6.º sejam puníveis como infrações penais.

2. Os Estados-Membros devem tomar as medidas necessárias para garantir que a tentativa de prática de uma das infrações previstas nos artigos 3.º a 6.º seja punível como infração penal.

Artigo 8.º
Sanções aplicáveis às pessoas singulares

1. Os Estados-Membros devem tomar as medidas necessárias para assegurar que as infrações previstas nos artigos 3.º a 7.º sejam puníveis com sanções penais efetivas, proporcionadas e dissuasoras.

2. Os Estados-Membros devem tomar as medidas necessárias para garantir que as infrações previstas nos artigos 3.º, 4.º e 5.º sejam puníveis com uma pena máxima de prisão não inferior a três anos.

3. Os Estados-Membros devem tomar as medidas necessárias para garantir que as infrações previstas no artigo 6.º sejam puníveis com uma pena máxima de prisão não inferior a dois anos.

4. Os Estados-Membros devem tomar as medidas necessárias para assegurar que as infrações previstas nos artigos 3.º, 4.º e 5.º sejam puníveis com uma pena máxima de prisão não inferior a cinco anos se:

(a) Forem cometidas no âmbito de uma organização criminosa, na aceção da Decisão-Quadro 2008/841/JAI, independentemente da sanção prevista nessa decisão;

(b) Causarem danos alargados ou consideráveis ou envolverem uma vantagem agregada de, pelo menos, 20 000 EUR.

Artigo 9.º
Responsabilidade das pessoas coletivas

1. Os Estados-Membros devem tomar as medidas necessárias para assegurar que as pessoas coletivas possam ser responsabilizadas pelas infrações previstas nos artigos 3.º a 7.º cometidas em seu benefício por qualquer pessoa, agindo a título individual ou como membro de um órgão da pessoa coletiva e que nela tenha uma posição proeminente, com base num dos seguintes elementos:

(a) No poder de representação da pessoa coletiva;

(b) No poder de tomar decisões em nome da pessoa coletiva;

(c) Na autoridade para exercer o controlo a nível dessa pessoa coletiva.

2. Os Estados-Membros devem tomar as medidas necessárias para assegurar que as pessoas coletivas possam ser responsabilizadas sempre que a falta de supervisão ou de controlo por parte de uma pessoa referida no n.º 1 tenha tornado possível a prática, por uma pessoa que lhe seja subordinada, das infrações previstas nos artigos 3.º a 7.º em benefício dessa pessoa coletiva.

3. A responsabilidade das pessoas coletivas por força dos n.os 1 e 2 não exclui a ação judicial contra as pessoas singulares que sejam autoras, instigadoras ou cúmplices de uma das infrações previstas nos artigos 3.º a 7.º.

Artigo 10.º
Sanções aplicáveis a pessoas coletivas

Os Estados-Membros tomam as medidas necessárias para assegurar que uma pessoa coletiva considerada responsável nos termos do artigo 9.º, n.º 1, seja sujeita a sanções efetivas, proporcionadas e dissuasoras, incluindo multas de caráter penal ou não penal e, eventualmente, outras sanções, tais como:

(a) A exclusão do direito a benefícios ou auxílios públicos;

(b) A interdição temporária ou definitiva do exercício de atividades comerciais;

(c) A sujeição a controlo judicial;

(d) A liquidação judicial;

(e) Encerramento temporário ou definitivo dos estabelecimentos utilizados para a prática da infração.

TÍTULO III: COMPETÊNCIA JURISDICIONAL E INVESTIGAÇÃO

Artigo 11.º
Competência jurisdicional

1. Cada Estado-Membro deve tomar as medidas necessárias para determinar a sua competência jurisdicional relativamente às infrações previstas nos artigos 3.º a 7.º, sempre que:

   (a) A infração tenha sido cometida, no todo ou em parte, no seu território;

   (b) O autor da infração penal seja um dos seus nacionais;

   (c) A infração causar danos no seu território, incluindo danos resultantes do roubo da identidade de uma pessoa.

2. Ao determinarem a sua competência jurisdicional nos termos do n.º 1, alínea a), os Estados-Membros devem assegurar que são competentes nos casos em que:

   (a) O autor praticou a infração quando se encontrava fisicamente presente no território desse Estado-Membro, independentemente de a infração ser cometida utilizando computadores ou um sistema de informação situado no seu território;

   (b) A infração tenha sido cometida utilizando computadores ou um sistema de informação situado no seu território, independentemente de o seu autor se encontrar ou não fisicamente presente nesse território.

3. Os Estados-Membros devem informar a Comissão caso decidam alargar a sua competência às infrações previstas nos artigos 3.º a 7.º cometidas fora do seu território, nomeadamente caso:

   (a) O autor tenha a sua residência habitual no seu território;

   (b) A infração tenha sido cometida em benefício de uma pessoa coletiva estabelecida no seu território;

   (c) O crime for cometido contra um dos seus nacionais ou contra uma pessoa que resida habitualmente no seu território.

Artigo 12.º
Investigações eficazes

1. Os Estados-Membros devem tomar as medidas necessárias para garantir que sejam disponibilizados instrumentos de investigação eficazes, como os utilizados nos casos de criminalidade organizada ou de outros crimes graves, às pessoas, às unidades ou

aos serviços responsáveis por investigar ou promover a ação penal no que respeita às infrações previstas nos artigos 3.º a 7.º.

2. Os Estados-Membros devem tomar as medidas necessárias para garantir que, quando o direito nacional obriga as pessoas singulares e coletivas a fornecer informações acerca das infrações previstas nos artigos 3.º a 7.º, essas informações cheguem sem atrasos indevidos às autoridades responsáveis por investigar ou agir penalmente contra essas infrações.

TÍTULO IV: INTERCÂMBIO DE INFORMAÇÕES E COMUNICAÇÃO DE INFORMAÇÕES SOBRE CRIMES

Artigo 13.º
Intercâmbio de informações

1. Para efeitos de intercâmbio de informações relativas às infrações previstas nos artigos 3.º a 7.º, os Estados-Membros devem assegurar a existência de um ponto de contacto operacional nacional disponível 24 horas por dia e sete dias por semana. Os Estados-Membros devem também assegurar a existência de procedimentos que permitam dar prontamente resposta a 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 objeto de resposta, bem como a forma e o prazo estimado de resposta. Os Estados-Membros podem decidir utilizar as redes de pontos de contacto operacionais existentes.

2. Os Estados-Membros devem informar a Comissão, a Europol e a Eurojust acerca dos pontos de contacto designados referidos no n.º 1. A Comissão transmite essa informação aos outros Estados-Membros.

Artigo 14.º
Comunicação de informações sobre crimes

1. Os Estados-Membros devem tomar as medidas necessárias para assegurar a disponibilização de canais de comunicação adequados para facilitar a comunicação sem atrasos indevidos das infrações previstas nos artigos 3.º a 7.º às autoridades policiais e a outras nacionais competentes.

2. Os Estados-Membros devem tomar as medidas necessárias para incentivar as instituições financeiras e outras pessoas coletivas que operem no seu território a comunicar sem atrasos indevidos informações sobre suspeitas de fraude às autoridades policiais e outras autoridades competentes, para efeitos de deteção, prevenção, investigação ou repressão das infrações previstas nos artigos 3.º a 7.º.

TÍTULO V: ASSISTÊNCIA ÀS VÍTIMAS E PREVENÇÃO

Artigo 15.º
Assistência e apoio às vítimas

1. Os Estados-Membros devem assegurar que todas as pessoas singulares e coletivas que tenham sido prejudicadas pelas infrações previstas nos artigos 3.º a 7.º, cometidas mediante a utilização abusiva de dados pessoais, têm acesso a informações e aconselhamento sobre como se podem proteger contra as consequências negativas das infrações, como por exemplo danos reputacionais.

2. Os Estados-Membros devem assegurar que todas as pessoas coletivas vítimas das infrações previstas nos artigos 3.º a 7.º da presente diretiva têm acesso, sem atrasos indevidos após o primeiro contacto com a autoridade competente, a informações sobre:

   (a) Os procedimentos para apresentação de denúncias relativas à infração e o seu papel no contexto desses procedimentos;

   (b) Os procedimentos disponíveis para apresentação de denúncias caso a autoridade competente não respeite os seus direitos no decurso dos processos penais;

   (c) Os contactos para o envio de comunicações relativas ao seu processo.

Artigo 16.º
Prevenção

Os Estados-Membros devem tomar as medidas adequadas, incluindo através da Internet, tais como campanhas de informação e sensibilização e programas de investigação e educação, se for caso disso em cooperação com as partes interessadas, com vista a reduzir globalmente a fraude, sensibilizar para estas questões e reduzir o risco de alguém se tornar vítima de fraude.

TÍTULO VI: DISPOSIÇÕES FINAIS

Artigo 17.º
Acompanhamento e estatísticas

1. O mais tardar até [3 meses após a entrada em vigor da presente diretiva], a Comissão deve criar um programa pormenorizado de acompanhamento dos resultados e dos impactos da presente diretiva. O programa de acompanhamento deve definir de que forma e em que intervalos os dados e as outras provas necessárias serão recolhidos. Deve especificar as medidas a tomar pela Comissão e pelos Estados-Membros aquando da recolha, partilha e análise dos dados e das outras provas.

2. Os Estados-Membros devem assegurar a criação de um sistema de registo, produção e disponibilização de dados estatísticos que reflitam as fases de comunicação de informações, investigação e ação judicial relativamente às infrações previstas nos artigos 3.º a 7.º.

3. Os dados estatísticos referidos no n.º 2 devem abranger, no mínimo, o número de infrações previstas nos artigos 3.º a 7.º comunicadas aos Estados-Membros, o número de casos investigados, o número de pessoas alvo de ação penal e condenadas pelas infrações previstas nos artigos 3.º a 7.º, bem como dados sobre o funcionamento da comunicação de informações.

4. Os Estados-Membros devem transmitir os dados recolhidos nos termos dos n.os 1, 2 e 3 à Comissão numa base anual. A Comissão deve assegurar a publicação anual de uma revisão consolidada destes relatórios estatísticos e a sua transmissão às agências e organismos especializados competentes da União.

Artigo 18.º
Substituição da Decisão-Quadro 2001/413/JAI

A Decisão-Quadro 2001/413/JAI é substituída relativamente aos Estados-Membros vinculados pela presente diretiva, sem prejuízo das obrigações desses Estados-Membros no que respeita ao prazo de transposição da referida decisão-quadro para o direito interno.

No que respeita aos Estados-Membros vinculados pela presente diretiva, as remissões para a Decisão-Quadro 2001/413/JAI devem ser entendidas como sendo feitas para a presente diretiva.

Artigo 19.º
Transposição

1. Os Estados-Membros devem pôr em vigor, até [24 meses após a entrada em vigor], as disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento à presente diretiva. Os Estados-Membros comunicam imediatamente à Comissão o texto dessas disposições.

2. Quando os Estados-Membros adotarem essas disposições, estas incluem uma referência à presente diretiva ou são acompanhadas dessa referência aquando da sua publicação oficial. As modalidades dessa remissão são estabelecidas pelos Estados-Membros.

3. Os Estados-Membros comunicam à Comissão o texto das medidas que adotarem no domínio regulado pela presente diretiva.

Artigo 20.º
Avaliação e relatórios

1. A Comissão deve, até [48 meses após a entrada em vigor], apresentar um relatório ao Parlamento Europeu e ao Conselho, no qual avalie em que medida os Estados-Membros tomaram as medidas necessárias para dar cumprimento à presente diretiva.

Os Estados-Membros transmitem à Comissão todas as informações necessárias para a elaboração do relatório.

2. A Comissão deve, até [96 meses após a entrada em vigor], realizar uma avaliação da presente diretiva relativa ao combate à fraude e à contrafação de meios de pagamento que não em numerário e apresentar um relatório ao Parlamento Europeu e ao Conselho.

Artigo 21.º
Entrada em vigor

A presente diretiva entra em vigor no vigésimo dia seguinte ao da sua publicação no Jornal Oficial da União Europeia.

Os destinatários da presente diretiva são os Estados-Membros, em conformidade com os Tratados.

Feito em Bruxelas, em

Pelo Parlamento Europeu
O Presidente

Pelo Conselho
O Presidente