Conseil de
l'Union européenne

**Bruxelles, le 14 septembre 2017**
**(OR. en)**

**12181/17**

**Dossier interinstitutionnel:**
**2017/0226 (COD)**

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

**PROPOSITION**

| | |
|---|---|
| Origine: | Pour le Secrétaire général de la Commission européenne, Monsieur Jordi AYET PUIGARNAU, Directeur |
| Date de réception: | 13 septembre 2017 |
| Destinataire: | Monsieur Jeppe TRANHOLM-MIKKELSEN, Secrétaire général du Conseil de l'Union européenne |
| N° doc. Cion: | COM(2017) 489 final |
| Objet: | Proposition de DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces et remplaçant la décision-cadre 2001/413/JAI du Conseil |

Les délégations trouveront ci-joint le document COM(2017) 489 final.

p.j.: COM(2017) 489 final

COMMISSION
EUROPÉENNE

Bruxelles, le 13.9.2017
COM(2017) 489 final

2017/0226 (COD)

Proposition de

# DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL

## concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces et remplaçant la décision-cadre 2001/413/JAI du Conseil

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

# TABLE DES MATIÈRES

# EXPOSÉ DES MOTIFS

## 1. CONTEXTE DE LA PROPOSITION

### 1.1. Motivation et objectifs de la proposition

La législation actuelle de l'UE qui établit des règles minimales communes pour incriminer la fraude aux moyens de paiements autres qu'en espèces est la décision-cadre 2001/413/JAI du Conseil concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces[1].

Le programme européen en matière de sécurité[2] reconnaît que la décision-cadre n'est plus en phase avec les réalités d'aujourd'hui et ne suffit plus pour faire face aux nouveaux défis et aux évolutions technologiques comme les monnaies virtuelles et les paiements mobiles.

En 2013, les fraudes aux cartes émises dans l'espace unique de paiement en euros (SEPA) ont atteint 1,44 milliard d'euros, soit une augmentation de 8 % par rapport à l'année précédente. Bien que les données relatives aux fraudes existent seulement pour les cartes de paiement, les cartes constituent le moyen de paiement autre que les espèces le plus important dans l'UE en termes de nombre de transactions[3].

Il importe de combattre efficacement la fraude aux moyens de paiement autres que les espèces car elle représente une menace pour la sécurité. Elle est source de revenus pour la criminalité organisée et donc propice à d'autres activités criminelles comme le terrorisme, le trafic de stupéfiants et la traite des êtres humains. Selon Europol, les revenus générés par ce type de fraude servent à financer:

- les voyages:
    - vols: l'expérience acquise lors des opérations menées de 2014 à 2016 dans le cadre du Global Airline Action Day[4] révèle un lien manifeste entre la fraude aux moyens de paiement autres que les espèces, la fraude aux billets d'avions et d'autres formes de grande criminalité organisée, y compris le terrorisme. Certaines personnes voyageant avec des billets obtenus frauduleusement étaient connues pour d'autres infractions ou suspectées d'y avoir participé;
    - autre fraude au voyage (vente et voyage avec des billets obtenus frauduleusement). Le principal moyen utilisé pour acheter des billets illicites était des cartes de crédit piratées. D'autres méthodes comprenaient, par exemple, l'utilisation de comptes de points de fidélité piratés, l'hameçonnage d'agences de voyage et la fraude aux bons. Outre les criminels, les personnes

---

1 Journal officiel L 149 du 2.6.2001, p.1.

2 Communication de la Commission intitulée «Stratégie pour un marché unique numérique en Europe», COM(2015) 192 final:

3 Banque centrale européenne, «*Fourth report on card fraud*», juillet 2015 (dernières données disponibles).

4 De plus amples détails sont disponibles ici.

qui voyageaient avec des billets obtenus frauduleusement incluaient des victimes de la traite des êtres humains et des personnes servant de «mules»[5];

- l'hébergement: les autorités répressives signalent aussi que la fraude aux moyens de paiement autres que les espèces est également utilisée pour faciliter d'autres infractions qui nécessitent un hébergement provisoire, comme la traite des êtres humains, l'immigration clandestine ou le trafic de stupéfiants.

Europol a en outre signalé que le marché de la fraude aux moyens de paiement autres que les espèces au sein de l'UE est dominé par des groupes de la criminalité organisée bien structurés et opérant au niveau mondial[6].

De plus, la fraude aux moyens de paiement autres que les espèces entrave le développement du marché unique numérique de deux manières:

- elle cause des pertes économiques directes considérables, comme l'indique le niveau susmentionné de 1,44 milliard d'euros estimé pour la fraude aux cartes de crédit. Par exemple, les compagnies aériennes imputent une perte annuelle à l'échelle mondiale d'environ 1 milliard de dollars à la fraude aux cartes[7];

- elle réduit la confiance des consommateurs, ce qui peut avoir pour conséquence de ralentir l'activité économique et d'affaiblir les investissements dans le marché unique numérique. Selon le dernier Eurobaromètre sur la cybersécurité[8], la grande majorité des utilisateurs d'internet (85 %) a le sentiment que le risque de devenir victime de cybercriminalité ne cesse d'augmenter. En outre, 42 % des utilisateurs s'inquiètent de la sécurité des paiements en ligne. 12 % sont moins enclins à effectuer des transactions numériques, comme utiliser les services bancaires en ligne, à cause de leurs craintes pour la sécurité.

Une évaluation du cadre législatif actuel de l'UE[9] a recensé trois problèmes qui sont à l'origine de la situation actuelle de la fraude aux moyens de paiement autres que les espèces dans l'UE:

1. certaines infractions ne peuvent pas faire l'objet d'**enquêtes et de poursuites effectives** avec le cadre juridique actuel;

2. certaines infractions ne peuvent pas faire l'objet d'**enquêtes et de poursuites effectives** à cause d'**obstacles opérationnels**;

3. les criminels profitent des lacunes de la **prévention** pour commettre les fraudes.

---

5 Le terme «mule» désigne une personne qui transfère des produits du crime entre différents pays. Les mules reçoivent le produit du crime sur leur compte; on leur demande ensuite de le retirer et de virer l'argent sur un compte différent, très souvent à l'étranger, en gardant une partie pour elles.

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

7 IATA, 2015.

8 Commission européenne, *Special Eurobarometer 423 — Cyber Security*, février 2015.

9 Document de travail des services de la Commission – Analyse d'impact accompagnant la proposition de directive concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces, SWD(2017)298.

La présente proposition a trois objectifs spécifiques pour résoudre les problèmes identifiés:

1. la mise en place d'une politique/d'un cadre juridique clair, solide et **technologiquement neutre**;

2. l'élimination des **obstacles opérationnels** qui entravent les enquêtes et les poursuites;

3. l'amélioration de la **prévention.**

### 1.2. Nécessité de mettre en œuvre les normes et obligations internationales pertinentes et de lutter de manière efficace contre la fraude et la contrefaçon des moyens de paiement autres que les espèces

La convention sur la cybercriminalité du Conseil de l'Europe (convention de Budapest)[10] , dans son titre 2 qui porte sur les infractions informatiques, fait obligation à chaque partie à la convention d'ériger en infraction pénale, conformément à son droit interne, la falsification informatique (article 7) et la fraude informatique (article 8). La décision-cadre actuelle est conforme à ces dispositions. La révision des règles actuelles aura pour effet d'améliorer la coopération au sein de la police et des autorités judiciaires et encore davantage entre les services répressifs et les entités privées, et contribuera par conséquent à réaliser les objectifs globaux de la convention, tout en restant compatible avec ses dispositions pertinentes.

### 1.3. Cohérence avec les dispositions existantes dans le domaine d'action

Les objectifs de la présente proposition sont compatibles avec la politique et les dispositions législatives en matière de droit pénal suivantes:

1. les **mécanismes de coopération paneuropéens en matière pénale** qui facilitent la coordination des enquêtes et des poursuites (procédure pénale):

   - décision-cadre 2002/584/JAI du Conseil relative au mandat d'arrêt européen et aux procédures de remise entre États membres[11];

   - convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne[12];

   - directive 2014/41/UE concernant la décision d'enquête européenne en matière pénale[13];

   - décision-cadre 2005/214/JAI du Conseil concernant l'application du principe de reconnaissance mutuelle aux sanctions pécuniaires[14];

---

10 Convention sur la cybercriminalité du Conseil de l'Europe (STE n° 185).

11 Décision-cadre 2002/584/JAI du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres

12 Acte du Conseil du 29 mai 2000 établissant, conformément à l'article 34 du traité sur l'Union européenne, la convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne

13 Directive 2014/41/UE du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale.

14 Décision-cadre 2005/214/JAI du Conseil du 24 février 2005 concernant l'application du principe de reconnaissance mutuelle aux sanctions pécuniaires.

- décision-cadre 2009/948/JAI du Conseil relative à la prévention et au règlement des conflits en matière d'exercice de la compétence dans le cadre des procédures pénales[15];

- décision-cadre 2009/315/JAI du Conseil concernant l'organisation et le contenu des échanges d'informations extraites du casier judiciaire entre les États membres[16];

- directive 2012/29/UE établissant des normes minimales concernant les droits, le soutien et la protection des victimes de la criminalité[17];

- règlement (UE) 2016/794 relatif à Europol[18];

- décision 2002/187/JAI du Conseil instituant Eurojust[19];

- conclusions du Conseil sur l'amélioration de la justice pénale dans le cyberespace[20];

Par principe, la proposition n'introduit pas de dispositions spécifiques à la fraude aux moyens de paiement autres que les espèces qui s'écarteraient de ces instruments d'une portée plus large, afin d'éviter la fragmentation qui pourrait compliquer la transposition et la mise en œuvre par les États membres. La seule exception réside dans la directive 2012/29/UE relative aux droits, au soutien et à la protection des victimes, que la présente proposition complète.

2. Actes juridiques qui **érigent en infractions pénales** des agissements liés à la fraude et la contrefaçon des moyens de paiement autres que les espèces (droit pénal positif):

- directive 2013/40/UE relative aux attaques contre les systèmes d'information[21]:

  - la présente proposition complète la directive 2013/40, en abordant un autre aspect de la cybercriminalité[22]. Les deux instruments correspondent à des

---

15 Décision-cadre 2009/948/JAI du Conseil du 30 novembre 2009 relative à la prévention et au règlement des conflits en matière d'exercice de la compétence dans le cadre des procédures pénales.

16 Décision-cadre 2009/315/JAI du Conseil du 26 février 2009 concernant l'organisation et le contenu des échanges d'informations extraites du casier judiciaire entre les États membres.

17 Directive 2012/29/UE du Parlement européen et du Conseil du 25 octobre 2012 établissant des normes minimales concernant les droits, le soutien et la protection des victimes de la criminalité et remplaçant la décision-cadre 2001/220/JAI du Conseil.

18 Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI

19 Décision 2002/187/JAI du Conseil du 28 février 2002 instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité

20 Conclusions du Conseil du 6 juin 2016 sur l'amélioration de la justice pénale dans le cyberespace.

21 Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil.

22 La stratégie de cybersécurité de l'UE indique qu'«on entend généralement par cybercriminalité un large éventail d'activités criminelles dont les ordinateurs et systèmes informatiques constituent soit l'arme soit la cible principale. La cybercriminalité recouvre les délits habituels (fraude, contrefaçon et usurpation d'identité p. ex.), les délits liés au contenu (distribution en ligne de matériel pédopornographique ou

ensembles distincts de dispositions de la convention de Budapest sur la cybercriminalité du Conseil de l'Europe[23], qui représente le cadre juridique international de référence pour l'UE[24];

- la présente proposition est en outre compatible avec la directive 2013/40 car elle repose sur une approche similaire pour des points spécifiques tels que la compétence ou la définition du niveau minimal des peines maximales;

- directive 2014/62/UE relative à la protection pénale de l'euro et des autres monnaies contre la contrefaçon[25]:

  - la présente proposition complète la directive 2014/62/UE car elle porte sur la contrefaçon des instruments de paiement autres que les espèces, tandis que la directive 2014/62/UE concerne la contrefaçon des espèces;

  - elle est en outre compatible avec la directive 2014/62/UE car elle applique la même approche pour certaines dispositions, par exemple celles relatives aux outils d'enquête;

- directive 2017/541/UE relative à la lutte contre le terrorisme:

  - la présente proposition complète la directive 2017/541/UE car elle vise à réduire le volume global des fonds obtenus par la fraude aux moyens de paiement autres que les espèces, dont la majeure partie aboutit dans les groupes de la criminalité organisée et leur permet de commettre des infractions graves, dont le terrorisme;

- la proposition de directive visant à combattre le blanchiment de capitaux grâce au droit pénal:

  - la présente proposition et la proposition de directive visant à combattre le blanchiment de capitaux grâce au droit pénal sont complémentaires en ce que la seconde crée le cadre juridique nécessaire pour réprimer à titre d'infraction principale le blanchiment des produits du crime que génère la fraude aux moyens de paiement autres que les espèces (grâce aux «mules»).

---

incitation à la haine raciale p. ex.) et les délits spécifiques aux ordinateurs et systèmes informatiques (attaque contre un système informatique, déni de service et logiciel malveillant p. ex.).

23 Convention sur la cybercriminalité du Conseil de l'Europe (STE n° 185). La directive 2013/40 correspond aux articles 2 à 6 de la convention, alors que la nouvelle initiative correspondrait aux articles 7 et 8 de la convention.

24 Commission et la Haute représentante de l'Union européenne pour les affaires étrangères et la politique de sécurité — Communication conjointe sur la stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé.

25 Directive 2014/62/UE du Parlement européen et du Conseil du 15 mai 2014 relative à la protection pénale de l'euro et des autres monnaies contre la contrefaçon, et remplaçant la décision-cadre 2000/383/JAI du Conseil.

### 1.4. Cohérence avec les autres politiques de l'UE

La présente proposition est cohérente avec le programme européen en matière de sécurité et avec la stratégie de cybersécurité de l'UE puisque ceux-ci ont pour objectif principal d'améliorer la sécurité.

En outre, elle est cohérente avec la stratégie du marché unique numérique qui vise à renforcer la confiance des utilisateurs dans le marché numérique, qui est un autre objectif principal de la proposition. Dans le contexte de la stratégie du marché unique numérique pour l'Europe, il existe plusieurs instruments juridiques pour faciliter les paiements sécurisés à travers l'UE, avec lesquels la présente proposition est aussi en cohérence:

- La directive révisée relative aux services de paiement (PSD2)[26] contient un nombre de mesures qui renforceront les exigences en matière de sécurité des paiements électroniques et créera un cadre juridique et de contrôle pour les acteurs émergents du marché des paiements;

- la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme (la «4e directive antiblanchiment»)[27] concerne le cas où les criminels abusent des instruments de paiement autres que les espèces dans le but de dissimuler leurs activités. La présente proposition complète la directive en régissant le cas où ces instruments de paiement ont, par exemple, été obtenus illégalement, contrefaits ou falsifiés par les criminels;

- proposition de directive modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme[28], dont la présente proposition reprend la définition des monnaies virtuelles. Si cette définition change au cours du processus d'adoption de la proposition précédente, il conviendrait d'adapter la définition de la présente proposition en conséquence;

- Les autres actes juridiques pertinents comprennent le règlement (UE) 2015/847 sur les informations accompagnant les transferts de fonds[29], le règlement (UE) nº 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur[30], le règlement (UE) 2012/260 établissant des exigences techniques et commerciales pour les virements et les

---

26 Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE, 2013/36/UE et le règlement (UE) nº 1093/2010, et abrogeant la directive 2007/64/CE.

27 Directive 2015/849/UE du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission.

28 Proposition de directive du Parlement européen et du Conseil modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme et modifiant la directive 2009/101/CE.

29 Règlement (UE) 2015/847 du Parlement européen et du Conseil du 20 mai 2015 sur les informations accompagnant les transferts de fonds et abrogeant le règlement (CE) n° 1781/2006.

30 Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

prélèvements en euros[31] et la directive (UE) 2012/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (directive NIS)[32].

En général, ces actes juridiques contribuent à la mise en place de mesures de prévention plus solides. La présente proposition les complète en ajoutant des mesures pour sanctionner les activités criminelles et permettre les poursuites là où la prévention a échoué.

## 2. BASE JURIDIQUE, SUBSIDIARITÉ ET PROPORTIONNALITÉ

### 2.1. Base juridique

La base juridique de l'action de l'UE est l'article 83, paragraphe 1, du traité sur le fonctionnement de l'Union européenne, qui mentionne expressément **la contrefaçon de moyens de paiement, la criminalité informatique et la criminalité organisée** parmi les domaines de criminalité particulièrement grave revêtant une dimension transfrontière:

*«Le Parlement européen et le Conseil, statuant par voie de directives conformément à la procédure législative ordinaire, peuvent établir des règles minimales relatives à la définition des infractions pénales et des sanctions dans des domaines de criminalité particulièrement grave revêtant une* ***dimension transfrontière*** *résultant du caractère ou des incidences de ces infractions ou d'un besoin particulier de les combattre sur des bases communes.*

*Ces domaines de criminalité sont les suivants: le terrorisme, la traite des êtres humains et l'exploitation sexuelle des femmes et des enfants, le trafic illicite de drogues, le trafic illicite d'armes, le blanchiment d'argent,* ***la corruption, la contrefaçon de moyens de paiement, la criminalité informatique et la criminalité organisée****...»*

### 2.2. Géométrie variable

La décision-cadre 2001/413/JAI concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces s'applique à tous les États membres.

Conformément au protocole n° 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé aux traités, le Royaume-Uni et l'Irlande peuvent décider de participer à l'adoption de la présente proposition. Ils disposent également de cette possibilité après l'adoption de la proposition.

Étant donné que le Royaume-Uni a notifié, le 29 mars 2017, son intention de quitter l'Union, conformément à l'article 50 du traité sur l'Union européenne (TUE), les traités cesseront de s'appliquer au Royaume-Uni à partir de la date d'entrée en vigueur de l'accord de retrait ou, à défaut, deux ans après la notification, sauf si le Conseil européen, en accord avec le

---

31 Règlement (UE) n° 260/2012 du Parlement européen et du Conseil du 14 mars 2012 établissant des exigences techniques et commerciales pour les virements et les prélèvements en euros et modifiant le règlement (CE) n° 924/2009

32 Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

Royaume-Uni, décide de proroger ce délai. En conséquence, et sans préjudice des dispositions de l'accord de retrait, la description précitée de la participation du Royaume-Uni à la présente proposition ne s'applique que jusqu'à ce que le Royaume-Uni cesse d'être un État membre.

En vertu du protocole n° 22 sur la position du Danemark, ce dernier ne participe pas à l'adoption, par le Conseil, des mesures visées au titre V du TFUE (à l'exception de la politique des visas). Par conséquent, en vertu des dispositions en vigueur, le Danemark ne prend pas part à l'adoption de la présente proposition et ne sera pas lié par elle.

### 2.3. Subsidiarité

La fraude aux moyens de paiement autres que les espèces revêt une très forte dimension internationale tant dans l'Union européenne qu'en dehors de cette dernière. Un cas typique est celui de la copie des données de la carte dans un pays de l'UE, la création ensuite d'une fausse carte à l'aide de ces données et le retrait de sommes d'argent avec cette fausse carte en dehors de l'UE pour contourner les normes de sécurité élevées. Ces délits ont de plus en plus souvent une dimension virtuelle.

Dès lors, l'objectif de lutter efficacement contre ces infractions ne peut pas être suffisamment réalisé par les États membres agissant de leur propre initiative et sans coordination:

- ces infractions créent des situations où la victime, l'auteur et la preuve peuvent tous relever de législations nationales différentes dans l'Union européenne et en-dehors de cette dernière. Par conséquent, lutter efficacement contre ces activités criminelles peut être très long et difficile pour un pays agissant seul, s'il n'existe pas de règles minimales communes;

- la nécessité d'une action de l'Union a déjà été reconnue du fait de l'élaboration de la législation européenne en vigueur pour lutter contre la fraude et la contrefaçon des moyens de paiement autres que les espèces (la décision-cadre).

- la nécessité d'une intervention de l'Union transparaît également dans les initiatives actuelles visant à coordonner au niveau de l'UE les mesures prises par les États membres dans ce domaine, comme la création d'une équipe Europol dédiée à la fraude aux moyens de paiement[33] et la priorité du cycle d'action EMPACT sur la coopération opérationnelle antifraude aux moyens de paiement autres que les espèces[34]. La valeur ajoutée de ces initiatives pour aider les États membres dans leur lutte contre ces infractions a été reconnue à maintes reprises lors de la consultation des parties intéressées réalisée dans la phase de préparation de la présente proposition, notamment pendant les réunions d'experts.

L'action de l'UE apporte une valeur ajoutée supplémentaire en facilitant la coopération avec les pays non membres de l'UE, étant donné que la dimension internationale de la fraude aux moyens de paiement autres que les espèces dépasse souvent les frontières de l'UE. L'existence de règles minimales communes au sein de l'UE peut aussi inspirer des solutions législatives efficaces aux pays non membres de l'UE, ce qui faciliterait la coopération transnationale au niveau mondial.

---

33 Voir le site web d'Europol.

34 De plus amples informations sont disponibles ici.

## 2.4. Proportionnalité

Conformément au principe de proportionnalité consacré à l'article 5, paragraphe 4, TUE, la nouvelle directive proposée est limitée à ce qui est nécessaire et proportionné pour mettre en œuvre les normes internationales et pour adapter aux nouvelles menaces la législation existante réprimant les infractions dans ce domaine. Les mesures relatives à l'utilisation des outils d'enquête et à l'échange des informations sont incluses uniquement dans la mesure nécessaire au bon fonctionnement du cadre juridique pénal proposé.

La proposition définit le champ des infractions pénales de façon à couvrir tous les agissements concernés, tout en le limitant à ce qui est nécessaire et proportionné.

## 2.5. Choix de l'instrument

Conformément à l'article 83, paragraphe 1, du TFUE, les règles minimales relatives à la définition des infractions pénales et des sanctions dans le domaine de la grande criminalité revêtant une dimension transfrontière, y compris la contrefaçon des moyens de paiement et la criminalité informatique, peuvent uniquement être établies par une directive du Parlement européen et du Conseil adoptée par la procédure législative ordinaire.

# 3. RÉSULTATS DES ÉVALUATIONS EX POST, DES CONSULTATIONS DES PARTIES INTÉRESSÉES ET DES ANALYSES D'IMPACT

## 3.1. Évaluations ex post/bilans de qualité de la législation existante

La Commission a réalisé une évaluation[35] du cadre législatif actuel de l'UE ainsi qu'une analyse d'impact, qui accompagne la présente proposition (voir le document de travail des services de la Commission correspondant pour de plus amples informations).

L'évaluation a décelé trois sources de problèmes, qui comportent chacune plusieurs facteurs:

[35] Document de travail des services de la Commission – Analyse d'impact accompagnant la proposition de directive concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces, SWD(2017)298.

| Sources de problèmes | Facteurs |
|---|---|
| 1. Certaines infractions ne peuvent pas faire l'objet d'**enquêtes et de poursuites effectives** avec le **cadre juridique** actuel. | a. Certaines infractions ne peuvent pas faire l'objet de poursuites effectives car les infractions commises avec certains instruments de paiement (en particulier **non matériels**) sont incriminées de diverses manières dans les États membres ou ne le sont pas.<br>b. Les **actes préparatoires** à la fraude aux moyens de paiement autres que les espèces ne peuvent pas faire l'objet de poursuites effectives car ils sont incriminés de diverses manières dans les États membres ou ne le sont pas.<br>c. Les enquêtes transfrontières peuvent être entravées parce qu'une même infraction est sanctionnée par **différents niveaux** de peine d'un État membre à l'autre.<br>d. L'absence de détermination de la **compétence** peut nuire à l'efficacité des enquêtes et des poursuites. |
| 2. Certaines infractions ne peuvent pas faire l'objet d'**enquêtes et de poursuites effectives** à cause d'**obstacles opérationnels**. | a. Le délai nécessaire pour obtenir des informations dans les demandes de **coopération transfrontière** peut être trop long, ce qui entrave l'enquête et les poursuites.<br>b. Le signalement insuffisant aux autorités répressives, à cause des contraintes de la **coopération public-privé**, nuit à l'efficacité des enquêtes et des poursuites. |
| 3. Les criminels profitent des lacunes de la **prévention** pour commettre les fraudes. | a. Le **partage d'informations** insuffisant dans la **coopération public-privé** nuit à la prévention.<br>b. Les criminels exploitent le **manque d'information** des victimes. |

Les sources de problèmes indiquent que l'on est en présence d'une **faille réglementaire,** le cadre juridique actuel de l'UE (la décision-cadre) étant devenu partiellement obsolète, principalement en raison des **progrès technologiques**. L'évaluation a montré que ce vide réglementaire n'avait pas été suffisamment comblé par les textes plus récents.

### 3.2. Consultation des parties intéressées

Processus de consultation:

Trois types de consultation ont été réalisés: une consultation publique, une consultation ciblée organisée par la Commission européenne et une consultation ciblée organisée par un prestataire.

1. Consultation publique

La Commission européenne a lancé une consultation publique le 1er mars 2017, en vue de recueillir les avis du public au sujet de la définition du problème, de la pertinence et de l'efficacité du cadre juridique actuel relatif à la fraude aux moyens de paiement autres que les espèces, ainsi que des solutions envisageables, et de leurs éventuels effets, pour résoudre les problèmes existants. La consultation a été clôturée au terme de 12 mois, le 24 mai 2017.

33 praticiens et 21 membres du public ont répondu aux questionnaires de la consultation. Quatre praticiens ont apporté une participation supplémentaire sous la forme de contributions écrites. Les praticiens étaient notamment:

- des entreprises privées (secteur privé);
- des autorités publiques internationales ou nationales (services répressifs, autorités judiciaires et institutions et organes de l'UE);
- des membres des milieux commerciaux, du monde des affaires ou d'associations professionnelles (par ex. fédérations bancaires nationales);
- des organisations non gouvernementales, des plateformes ou des réseaux;
- des consultants professionnels, des cabinets d'avocats, des consultants indépendants.

2. Consultation ciblée organisée par la Commission européenne:

- grandes réunions d'experts rassemblant des représentants de la police et de l'ordre judiciaire de tous les pays de l'UE (sélectionnés par les États membres) et des experts du secteur privé (établissements financiers, prestataires de services de paiement, commerçants, systèmes de cartes de paiement);
- diverses réunions avec des experts et des acteurs des milieux universitaires, des services répressifs, du secteur des monnaies virtuelles, et des représentants des organisations de consommateurs, des établissements financiers privés et des régulateurs financiers.

3. Consultation ciblée organisée par un prestataire:

Un prestataire a organisé des consultations ciblées comprenant des sondages et des entretiens en ligne. Les résultats préliminaires ont été présentés à un groupe de concertation et de validation qui a ensuite donné son avis et vérifié les résultats de la consultation.

En tout, 125 parties intéressées de 25 États membres ont répondu.

Principaux résultats:

- Ampleur de la criminalité:

  les coûts liés à la fraude aux moyens de paiement autres que les espèces sont généralement perçus comme élevés et devraient encore croître au cours des prochaines années. Lorsqu'on leur a demandé de quantifier le phénomène de la criminalité, toutes les parties intéressées, de toutes les catégories, ont estimé cela difficile. Les statistiques sont rares et pas toujours accessibles. Toutefois, certaines statistiques apportaient des éléments concrets confirmant l'ampleur de certains types de fraude aux moyens de paiement autres que les espèces.

- Cadre juridique pénal:

  la plupart des parties intéressées considéraient que le présent cadre juridique de l'UE ne répond qu'en partie aux besoins de sécurité actuels, surtout pour ce qui concerne la définition des instruments de paiement et des infractions pénales. Certains ont confirmé que les cadres juridiques nationaux devraient être modifiés.

- Procédure pénale:

  malgré le cadre juridique existant, le degré actuel de coopération entre les États membres pour les enquêtes et les poursuites était jugé seulement partiellement satisfaisant. Le soutien apporté par Europol pour faciliter la coopération transfrontière a été largement reconnu.

- Signalement aux autorités répressives:

  les avis sur le signalement des infractions aux autorités répressives étaient variables: certains étaient satisfaits du taux actuel de signalement, tandis que d'autres estimaient qu'il devait être amélioré. Les différentes catégories de parties intéressées s'accordaient sur le fait que les futures options d'action en la matière devaient être conciliées avec les capacités réelles des services répressifs de suivre les affaires.

- Coopération public-privé:

  les parties intéressées estiment que la coopération entre le public et le privé est bénéfique dans l'ensemble et conviennent qu'elle doit être encouragée pour mieux lutter contre la fraude aux moyens de paiement autres que les espèces, surtout lorsqu'il s'agit de prévention.

  La plupart considèrent que cette coopération doit être intensifiée pour combattre ce type de fraude. Les représentants du secteur privé paraissaient les plus insatisfaits. Selon eux, les principaux obstacles à la coopération sont, par exemple, la possibilité limitée de partager des informations avec les services répressifs et l'insuffisance des outils servant à permettre ces échanges.

  La grande majorité des parties intéressées convient que, pour mener les enquêtes et engager des poursuites contre les criminels, il faut autoriser les établissements financiers à partager spontanément avec la police nationale ou la police d'un autre pays de l'UE certaines informations à caractère personnel (par ex. nom, compte bancaire, adresse, etc.) sur les victimes.

  Plusieurs parties intéressées ont également fait mention d'une mauvaise coopération entre les autorités privées et publiques parmi les obstacles à la fraude aux moyens de paiement autres que les espèces.

  Selon les entreprises privées, les autorités publiques, les milieux commerciaux, le monde des affaires et les associations professionnelles, la législation, les conflits entre priorités et un manque de confiance, ajoutés à des problèmes pratiques et organisationnels, constituent des obstacles à une coopération fructueuse entre autorités publiques et entités privées lorsque les participants sont établis dans des États membres différents. Le manque de moyens technologiques appropriés (par exemple, un canal de communication) était mentionné parmi les obstacles par les entreprises privées et les autorités publiques.

- Droits des victimes:

  les parties intéressées ont souligné l'importance de protéger les victimes de la fraude. Certaines estiment que les victimes ne bénéficient pas d'une protection suffisante, même si les initiatives prises par les États membres pour assurer une protection sont appréciées. Les associations de victimes ont établi de bons mécanismes de coopération avec les services répressifs. Plusieurs parties intéressées jugent nécessaire de mieux protéger les victimes contre les usurpations d'identité qui, selon elles, touchent aussi bien les personnes physiques que les personnes morales. Il y a donc lieu de protéger les victimes, quelle que soit leur nature juridique.

### 3.3. Analyse d'impact

Conformément à ses lignes directrices pour une meilleure réglementation[36], la Commission a réalisé une analyse d'impact[37] pour évaluer la nécessité de présenter une proposition législative.

L'analyse d'impact a été présentée et discutée avec le comité d'examen de la réglementation (CER) le 12 juillet 2017. Le comité a reconnu les efforts faits pour quantifier les coûts et les avantages. Il a rendu un avis positif[38], tout en recommandant d'améliorer encore le rapport sur les aspects suivants:

1. le rapport n'expliquait pas suffisamment le contexte, notamment le lien et la complémentarité avec les mécanismes existants et envisagés de coopération judiciaire et paneuropéenne;

2. l'objectif de l'initiative relatif à la croissance semblait surévalué.

Le rapport de l'analyse d'impact a été révisé en tenant compte des recommandations formulées par le comité dans son avis positif.

Après un recensement des mesures d'action possibles pour résoudre chaque problème identifié dans l'évaluation, et un examen de celles à retenir et celles à écarter, les mesures ont été regroupées en options d'action. Chaque option d'action a été élaborée de manière à résoudre les problèmes identifiés. Les différentes options retenues étaient cumulatives, c'est-à-dire que le degré d'action législative de l'UE allait croissant. Étant donné que le problème en cause est essentiellement dû à une **faille réglementaire**, il importait d'exposer tous les outils réglementaires pour déterminer l'action de l'UE qui serait la plus proportionnée.

Les différentes options examinées étaient les suivantes:

---

36 De plus amples informations sur les lignes directrices pour une meilleure réglementation sont disponibles ici.

37 Document de travail des services de la Commission – Analyse d'impact accompagnant la proposition de directive concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces, SWD(2017)298.

38 Comité d'examen de la réglementation de la Commission européenne – Opinion on the Impact Assessment – Combating fraud and counterfeiting of non-cash means of payment (en anglais uniquement), SEC(2017)390.

- **option A**: améliorer la mise en œuvre de la législation de l'UE et faciliter l'autorégulation pour la coopération public-privé ;

- **option B:** introduire un nouveau cadre législatif et faciliter l'autorégulation pour la coopération public-privé ;

- **option C:** identique à l'option B, mais en ajoutant des dispositions encourageant à faire rapport pour la coopération public-privé, au lieu de l'autorégulation, et de nouvelles dispositions relatives à la sensibilisation du public;

- **option D:** identique à l'option C, mais en ajoutant des dispositions sur la compétence juridictionnelle qui complètent les règles relatives à la décision d'enquête européenne et aux injonctions.

**L'option C était l'option privilégiée**, tant du point de vue qualitatif qu'en termes de coûts et avantages.

S'agissant des avantages, l'option privilégiée favoriserait une action répressive plus efficace et efficiente contre la fraude aux moyens de paiement autres que les espèces, grâce à une application plus cohérente des règles dans toute l'Union, une meilleure coopération transfrontière, davantage de coopération public-privé et d'échanges d'informations. L'initiative développerait également la confiance dans le marché unique numérique, en renforçant la sécurité.

S'agissant des coûts, le coût qu'entraîneraient, pour les États membres, l'élaboration et la réalisation d'une nouvelle initiative est estimé à environ 561 000 EUR (coût ponctuel). Les coûts permanents de mise en œuvre et de contrôle de l'application, pour les États membres, sont estimés à environ 2 285 140 EUR par an (total pour l'ensemble des États membres).

La proposition ne prévoyant aucune règle obligatoire concernant les rapports, elle ne devrait pas avoir d'incidence en matière de coûts supplémentaires pour les entreprises, notamment les PME. Les autres dispositions qui seraient incluses dans la proposition ne toucheraient pas non plus les PME.

Globalement, l'incidence cumulée des mesures proposées sur les coûts administratifs et financiers devrait être supérieure au niveau actuel car le nombre d'enquêtes à mener grèverait les ressources des services répressifs dans ce domaine, qui devraient être augmentées. Les principales raisons en sont les suivantes:

- la définition plus large des moyens de paiement et les infractions supplémentaires à traiter (actes préparatoires) risquent d'augmenter le nombre d'affaires dont la police et les autorités judiciaires seront chargées;

- des ressources supplémentaires seront nécessaires pour renforcer la coopération transfrontière;

- l'obligation des États membres d'établir des statistiques créera une charge administrative supplémentaire

En revanche, la mise en place d'un cadre juridique bien défini pour s'attaquer aux facteurs propices à la fraude aux moyens de paiement autres que les espèces permettrait de détecter, de

poursuivre et de sanctionner les activités afférentes à cette fraude à un stade plus précoce. De plus, si la coopération public-privé grève certes les ressources, le «retour sur investissement» en termes d'efficacité et d'efficience de l'action répressive est immédiat.

### 3.4. Réglementation affûtée et simplification

Du point de vue qualitatif, la présente proposition est susceptible d'apporter des simplifications dans quelques domaines, par exemple:

- un plus grand rapprochement des législations pénales nationales (par exemple, en établissant des définitions communes et un niveau minimal commun de sanction pour les peines maximales) simplifierait et faciliterait la coopération entre les services répressifs nationaux qui enquêtent sur des affaires transfrontières et exercent les poursuites dans leur cadre;

- en particulier, des règles de compétence plus claires, un rôle plus important et renforcé pour les points de contact nationaux et le partage de données et d'informations entre les polices nationales et avec Europol pourraient simplifier davantage les procédures et les pratiques en matière de coopération.

Il n'est pas possible de quantifier ce potentiel de simplification en raison de l'absence de données (et, dans certains cas, de l'impossibilité d'isoler les effets de la décision-cadre).

Globalement, le potentiel de réglementation affûtée de la présente initiative est très limité:

1. premièrement, la décision-cadre de 2001 est déjà un acte juridique relativement simple qui offre peu de possibilité d'être simplifié davantage.

2. Deuxièmement, cette initiative vise à accroître la sécurité en comblant les lacunes actuelles. Cela entraînerait normalement une hausse des coûts administratifs, pour mener des enquêtes et exercer des poursuites contre des infractions qui ne sont actuellement pas couvertes, plutôt que les économies substantielles qui résulteraient d'une simplification de la coopération transfrontière.

3. Troisièmement, l'initiative n'a pas pour but d'imposer des obligations juridiques supplémentaires aux entreprises et aux citoyens. Elle demande aux États membres d'encourager et de faciliter le signalement des infractions par des canaux de communication appropriées (plutôt que d'imposer un signalement obligatoire), conformément aux autres instruments de l'UE tels que la directive 2011/93 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie (article 16, paragraphe 2).

### 3.5. Droits fondamentaux

La proposition inclut des dispositions destinées à adapter le cadre juridique de la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces aux menaces nouvelles et émergentes et à régir les formes de cette fraude qui ne sont pas couvertes à l'heure actuelle.

L'objectif ultime de ces mesures est de protéger les droits des victimes effectives et potentielles. L'instauration d'un cadre juridique bien défini permettant aux autorités policières et judiciaires de réprimer les activités criminelles qui touchent directement les données à

caractère personnel des victimes, par exemple l'incrimination des actes préparatoires, pourrait notamment améliorer la protection du droit des victimes effectives et potentielles à la vie privée et à la protection de leurs données à caractère personnel.

En même temps, toutes les mesures prévues dans la présente proposition respectent les droits et libertés fondamentaux reconnus dans la charte des droits fondamentaux de l'Union européenne, et doivent être mises en œuvre en conséquence. Toute limitation de l'exercice de ces droits et libertés fondamentaux est soumise aux conditions énoncées à l'article 52, paragraphe 1, de la charte, c'est-à-dire qu'elle doit satisfaire au principe de proportionnalité au regard de la finalité légitime de répondre effectivement à des objectifs d'intérêt général reconnus par l'Union et au besoin de protection des droits et libertés d'autrui. De telles limitations doivent être prévues par la loi et respecter le contenu essentiel desdits droits et libertés.

À cet égard, divers droits et libertés fondamentaux consacrés par la charte ont été pris en compte, notamment: le droit à la liberté et à la sûreté le respect de la vie privée et familiale la liberté professionnelle et le droit de travailler la liberté d'entreprise le droit de propriété le droit à un recours effectif et à accéder à un tribunal impartial la présomption d'innocence et les droits de la défense les principes de légalité et de proportionnalité des délits et des peines ainsi que le droit à ne pas être jugé ou puni pénalement deux fois pour une même infraction.

La présente proposition respecte en particulier le principe de légalité et de proportionnalité des délits et des peines. Elle limite le champ des infractions à ce qui est nécessaire pour permettre de poursuivre effectivement les actes qui constituent une menace particulière pour la sécurité et elle introduit des règles minimales concernant le niveau des sanctions, dans le respect du principe de proportionnalité, en fonction de la nature de l'infraction.

La présente proposition vise en outre à assurer que les données relatives aux personnes soupçonnées d'avoir commis les infractions énumérées dans la présente directive soient traitées en respectant le droit fondamental à la protection des données à caractère personnel et la législation en vigueur, notamment dans le contexte de la coopération public-privé.

## 4. INCIDENCE BUDGÉTAIRE

La présente proposition n'a aucune incidence immédiate sur le budget de l'Union.

## 5. AUTRES ÉLÉMENTS

### 5.1. Plans de mise en œuvre et modalités de suivi, d'évaluation et d'information

La Commission surveillera la mise en œuvre de la directive sur la base des informations, fournies par les États membres, relatives aux mesures adoptées pour mettre en vigueur les dispositions législatives, réglementaires et administratives nécessaires afin de se conformer à la directive.

Deux ans après le délai de mise en œuvre de la présente directive, la Commission présentera au Parlement européen et au Conseil un rapport évaluant dans quelle mesure les États membres auront pris les mesures nécessaires pour se conformer à la présente directive.

En outre, la Commission procèdera à une évaluation des effets de la directive six ans après le délai de sa mise en œuvre, de façon à donner suffisamment de temps pour apprécier les effets de l'initiative après sa mise en œuvre complète dans tous les États membres.

### 5.2. Documents explicatifs

Aucun document explicatif sur la transposition n'est jugé nécessaire.

## 6. ÉLÉMENTS JURIDIQUES DE LA PROPOSITION

### 6.1. Résumé de l'action proposée

Tout en abrogeant la décision-cadre 2001/413/JAI, la présente proposition actualise la plupart de ses dispositions actuelles et elle tient compte des conclusions de l'évaluation et de l'analyse d'impact (par exemple, en ce qui concerne l'option privilégiée).

Le tableau ci-dessous indique les correspondances entre la proposition et la décision-cadre ainsi que les articles qui sont nouveaux et ceux qui ont été actualisés par rapport à cette dernière.

| | DIRECTIVE | | DÉCISION-CADRE | | Commentaires |
|---|---|---|---|---|---|
| | **Article** | **Considérant** | **Article** | **Considérant** | |
| I. Objet et définitions | 1. Objet | 1-6 | Aucun | 1-7 | Nouveau |
| | 2. Définitions | 7-8 | 1. Définitions | 10 | Actualisé |
| II. Infractions | 3. Utilisation frauduleuse des instruments de paiement | 9 | 2. Infractions liées aux instruments de paiement | 8-10 | |
| | 4. Infractions préparatoires à l'utilisation frauduleuse d'instruments de paiement | | | | |
| | 5. Infractions liées aux systèmes d'information | | 3. Infractions liées à l'utilisation de l'informatique | | |
| | 6. Outils utilisés pour commettre les infractions | | 4. Infractions liées aux équipements spécialement adaptés | | |
| | 7. Instigation, complicité et tentative | | 5. Participation, incitation et tentative | | |
| | 8. Sanctions à l'encontre des personnes physiques | 10-11 | 6. Sanctions | 9 | |
| | 9. Responsabilité des personnes morales | Aucun | 7. Responsabilité des personnes morales | Aucun | |
| | 10. Sanctions à l'encontre des personnes morales | | 8. Sanctions à l'encontre des personnes morales | | |
| III. Compétence juridictionnelle et enquêtes | 11. Compétence | 12-14 | 9. Compétence juridictionnelle<br>10. Extradition et poursuites | 11 | |
| | 12. Efficacité des enquêtes | 15 | Aucun | Aucun | Nouveau |
| IV. Échange d'informations et signalement des infractions | 13. Échange d'informations | 16-18 | 11. Coopération entre États membres<br>12. Échange d'informations | 11 | Actualisé |
| | 14. Signalement des infractions | 19 | Aucun | Aucun | Nouveau |
| V. Aide et soutien aux victimes et prévention | 15. Aide et soutien aux victimes | 20-22 | Aucun | | |
| | 16. Prévention | 23 | Aucun | | |
| VI. Dispositions finales | 17. Suivi et statistiques | 24 | Aucun | | |
| | 18. Remplacement de la décision-cadre | 25 | Aucun | | |
| | 19. Transposition | Aucun | 14. Mise en œuvre (paragraphe 1) | | Actualisé |
| | 20. Évaluation et rapport | | 14. Mise en œuvre [14(2)] | | |
| | 21. Entrée en vigueur | | 15. Entrée en vigueur | | |

| | | | | | |
|---|---|---|---|---|---|
| | Aucun | 26-29 | 13. Application territoriale | | Supprimé |

Concrètement, la présente proposition:

- définit les instruments de paiement d'une manière plus large et plus rigoureuse qui englobe également les instruments de paiement non matériels, ainsi que les instruments d'échange numériques;

- érige en infraction autonome, parallèlement à l'utilisation de ces instruments, la possession, la vente, l'obtention aux fins d'utilisation, l'importation, la diffusion ou toute autre forme de mise à disposition d'un instrument de paiement faux ou falsifié, volé ou approprié par d'autres moyens illégaux;

- élargit le champ des infractions liées aux systèmes d'information pour y inclure toutes les opérations de paiement, y compris celles réalisées au moyen d'instruments d'échange numériques;

- introduit des règles relatives au niveau des peines, en particulier pour fixer un niveau minimal pour les peines maximales;

- prévoit des infractions aggravées pour:

- les situations où les actes délictueux sont commis dans le cadre d'une organisation criminelle au sens de la décision-cadre 2008/841/JAI, indépendamment de la sanction qui y est prévue;

- les situations où l'acte délictueux cause un préjudice global considérable ou procure à ses auteurs un avantage économique considérable. Cette mesure vise à réprimer les cas où la fraude cause un faible préjudice individuel mais à un grand nombre de victimes, en particulier dans les transactions à distance («card-not-present»);

- précise l'étendue de la compétence juridictionnelle concernant les infractions visées dans la proposition, en donnant compétence aux États membres lorsque soit l'infraction a été commise à l'aide d'un système d'information situé sur le territoire d'un État membre alors que l'auteur se trouvait ailleurs, soit l'auteur se trouvait sur le territoire d'un État membre mais le système d'information était situé ailleurs;

- précise la portée de la compétence juridictionnelle au regard des effets de l'infraction, en permettant aux États membres d'exercer leur compétence si l'infraction cause un préjudice sur leur territoire, y compris à la suite d'une usurpation d'identité;

- introduit des mesures pour améliorer la coopération en matière de justice pénale à l'échelle de l'Union, en renforçant la structure existante et le recours aux points de contact opérationnels;

- améliore les conditions pour que les victimes et les entités privées signalent les infractions;

- répond au besoin d'établir des statistiques sur la fraude et la contrefaçon des moyens de paiement autres que les espèces, en obligeant les États membres à

veiller à la mise en place d'un système adapté pour enregistrer, produire et communiquer des statistiques sur les infractions visées dans la proposition de directive;

- offre aux victimes la possibilité d'obtenir des informations sur leurs droits et sur l'aide et le soutien disponibles, même si leur pays de résidence est différent de celui de l'auteur de la fraude ou de celui dans lequel l'enquête judiciaire est menée.

### 6.2. Explication détaillée des différentes dispositions de la proposition

*Article 1er: Objet* — cet article définit le champ d'application et l'objet de la proposition.

*Article 2: Définitions* — cet article établit les définitions pour tout l'instrument. L'article 2 reprend la définition des monnaies virtuelles qui figure dans la proposition de directive du Parlement européen et du Conseil modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme et modifiant la directive 2009/101/CE[39]. Si cette définition change au cours du processus d'adoption de ladite proposition, il conviendrait d'adapter en conséquence la définition des monnaies virtuelles dans le présent article.

*Article 3: Utilisation frauduleuse des instruments de paiement* — cet article énumère les infractions liées à des agissements délictueux qui constituent directement et immédiatement une fraude, à savoir l'utilisation frauduleuse d'instruments de paiement, y compris d'instruments volés et faux. Les infractions concernent tous les instruments de paiement, matériels ou non, et comprennent donc les fraudes commises à l'aide d'authentifiants de paiement volés ou falsifiés ou d'autres informations enregistrées permettant d'initier un ordre de paiement ou un autre transfert monétaire, y compris les transferts de monnaies virtuelles.

*Article 4: Infractions préparatoires à l'utilisation frauduleuse d'instruments de paiement* — cet article concerne des infractions liées à des agissements délictueux qui, tout en ne constituant pas immédiatement la fraude qui conduit à la perte d'un bien, sont commises pour préparer une fraude. Il s'agit notamment du vol ou de la contrefaçon d'un instrument de paiement et de divers actes intervenant dans le trafic de ces instruments volés ou faux. Sont comprises la possession, la diffusion ou la mise à disposition des instruments en vue d'une utilisation frauduleuse, notamment lorsque l'auteur a connaissance de la possibilité d'une telle utilisation (*dolus eventualis*). Comme l'article 3, cet article englobe toutes les infractions impliquant des instruments de paiement, matériels ou non, et concerne donc aussi les agissements tels que le commerce d'authentifiants volés («carding») et l'hameçonnage («phishing»)[40].

*Article 5: Infractions liées aux systèmes d'information* — cet article a trait à des actes délictueux liés aux systèmes d'information que les États membres doivent incriminer. La liste contient des éléments qui distinguent ces infractions de l'atteinte illégale à l'intégrité d'un

---

39 COM(2016) 450 final.

40 Le phishing ou hameçonnage est une méthode utilisée par les fraudeurs pour accéder aux informations personnelles intéressantes, comme les noms d'utilisateur et les mots de passe. Le plus souvent, un courrier électronique qui paraît provenir d'une société bien connue et de confiance est envoyé à une grande liste d'adresses électroniques. Ce courrier électronique peut aiguiller le destinataire vers un faux site web où on lui demande de fournir des informations personnelles.

système et de l'atteinte illégale à l'intégrité des données, prévues par la directive 2013/40/UE, comme le transfert de valeurs monétaires aux fins d'obtenir un gain illicite. Cette disposition a été incluse pour incriminer des agissements tels que le piratage de l'ordinateur ou d'un appareil d'une victime en vue de la rediriger vers un faux site web bancaire en ligne, de sorte que la victime effectue un paiement sur un compte bancaire contrôlé par le fraudeur (et devienne ainsi une «mule»)[41]. Elle couvre également d'autres types d'agissements délictueux, tels que le dévoiement («pharming»)[42], qui exploitent les systèmes d'information pour procurer un gain illicite à l'auteur ou à une autre personne.

*Article 6: Outils utilisés pour commettre les infractions* — cet article porte sur des infractions liées à des outils utilisés pour commettre les infractions mentionnées à l'article 4, points a) et b), et à l'article 5, et que les États membres doivent incriminer. Il vise à incriminer la production, la vente, l'obtention aux fins d'utilisation, l'importation, la diffusion ou toute autre forme de mise à disposition, lorsqu'elles sont intentionnelles, de copieurs de carte servant à voler les authentifiants, par exemple, ainsi que de logiciels malveillants et de faux sites web servant à l'hameçonnage. Cet article est largement inspiré de l'article 4 de la décision-cadre 2001/413/JAI et de l'article 3, point d), sous i), de la directive 2014/62/UE relative à la protection pénale de l'euro et des autres monnaies contre la contrefaçon.

*Article 7: Instigation, complicité et tentative* — cet article s'applique aux agissements liés aux infractions visées aux articles 3 à 6 et oblige les États membres à incriminer toute forme de préparation et de participation. La responsabilité pénale pour tentative est incluse pour les infractions visées aux articles 3 à 6.

*Article 8: Sanctions à l'encontre des personnes physiques* — pour lutter efficacement contre la fraude et la contrefaçon des moyens de paiement autres que les espèces, il faut que les sanctions soient dissuasives dans tous les États membres. Comme d'autres instruments de l'Union visant à rapprocher le niveau des sanctions pénales, cet article énonce que la peine maximale prévue par le droit national doit être d'au moins trois ans de prison, sauf pour les infractions prévues à l'article 6, pour lesquelles les peines maximales doivent être d'au moins deux ans. Il prévoit des peines plus sévères pour les infractions aggravées, à savoir une peine maximale d'au moins cinq ans lorsque l'infraction est commise par une organisation criminelle, au sens de la décision-cadre 2008/841/JAI du Conseil du 24 octobre 2008 relative à la lutte contre la criminalité organisée[43], ou lorsqu'elle est commise à grande échelle, causant ainsi un préjudice grave ou considérable, en particulier dans le cas où le préjudice individuel est faible mais touche globalement un grand nombre de victimes, ou lorsqu'une infraction procure à son auteur un avantage cumulé égal à au moins 20 000 EUR.

Il semble que les infractions mentionnées aux articles 2 à 5 de la décision-cadre 2001/413/JAI soient sanctionnées par des peines spécifiques dans la plupart des États membres où des informations étaient disponibles. Cependant, en général, il n'y a pas eu de rapprochement: si tous les États membres prévoient des peines privatives de liberté (au moins dans les cas

---

41 Le terme «mule» désigne une personne qui transfère des produits du crime entre différents pays. Les mules reçoivent le produit du crime sur leur compte; on leur demande ensuite de le retirer et de virer l'argent sur un compte différent, très souvent à l'étranger, en gardant une partie pour elles (ActionFraudUK, 2017). Soit elles savent que les fonds sont des produits du crime, soit elles sont amenées à croire qu'ils ont une origine légitime.

42 Le dévoiement («pharming») est une technique de piratage qui consiste à installer un code malveillant sur ordinateur personnel ou un serveur, qui détourne les utilisateurs vers des sites web frauduleux sans qu'ils s'en aperçoivent ou sans leur consentement.

43 JO L 300 du 11.11.2008, p. 42.

graves), le niveau des sanctions pour les mêmes agissements varie sensiblement. L'effet dissuasif est dès lors plus faible dans certains États membres que dans d'autres.

Les disparités de niveau de sanction risquent en outre de nuire à la coopération judiciaire. Si le code pénal d'un État membre prévoit une peine minimale peu élevée, la police et les autorités judiciaires n'accorderont pas une grande priorité aux enquêtes et aux poursuites concernant la fraude aux cartes bancaires dans les transactions à distance. Cela peut, à son tour, entraver la coopération transfrontière, lorsqu'un autre État membre sollicite de l'aide, lorsqu'il s'agit de traiter sa demande à temps. Ceux qui profiteront le plus de ces disparités de niveau de sanction seront probablement ceux qui commettent les infractions les plus graves, c'est-à-dire les groupes de la criminalité organisée transnationale, qui possèdent des bases d'action dans plusieurs États membres.

*Articles 9 et 10: Responsabilité des personnes morales et sanctions à leur encontre* — ces articles s'appliquent à toutes les infractions visées aux articles 3 à 7. Ils obligent les États membres à veiller à la responsabilité des personnes morales, sans exclure celle des personnes physiques, et à appliquer aux premières des sanctions effectives, proportionnées et dissuasives. L'article 10 énumère des exemples de sanctions.

*Article 11: Compétence juridictionnelle* — fondé sur les principes de territorialité et de personnalité, cet article énonce les situations dans lesquelles les États membres doivent établir leur compétence à l'égard des infractions mentionnées aux articles 3 à 7.

Il reprend des éléments de l'article 12 de la directive 2013/40/UE relative aux attaques contre les systèmes d'information. Lorsqu'une fraude ou une contrefaçon des moyens de paiement autres que les espèces a lieu en ligne, l'infraction est susceptible de s'étendre sur plusieurs pays: elle est souvent commise à l'aide de systèmes d'information situés hors du territoire sur lequel l'auteur est physiquement présent et elle a des conséquences dans un autre pays dans lequel les preuves peuvent également se trouver. L'article 11 vise ainsi à garantir que la compétence territoriale couvre les situations dans lesquelles l'auteur et le système d'information qu'il a utilisé pour commettre l'infraction sont situés sur des territoires différents.

Il intègre un nouvel élément qui répond au besoin d'affirmer la compétence si le préjudice est causé dans un pays autre que celui dans lequel les agissements ont eu lieu, notamment le préjudice consécutif à l'usurpation de l'identité d'une personne. Le but est de régir les situations qui ne relèvent pas de la directive 2013/40/UE relative aux attaques contre les systèmes d'information, et qui sont communes aux infractions ayant trait à la fraude aux moyens de paiement autres que les espèces. Il s'agit notamment des cas dans lesquels aucune des infractions associées à l'infraction en cause (par exemple, le vol des authentifiants d'une carte, le clonage d'une carte, un retrait illégal à un guichet automatique) n'a été commise dans l'État membre où le préjudice survient (par exemple, là où la victime a le compte bancaire sur lequel l'argent a été volé). Dans ces cas, la victime signalera le plus souvent l'incident aux autorités de l'État membre dans lequel le préjudice économique a été découvert. Cet État membre doit pouvoir exercer sa compétence pour qu'il y ait bien enquête et poursuites, comme point de départ d'investigations qui pourraient s'étendre à de multiples États membres et pays tiers.

*Article 12: Efficacité des enquêtes* — cet article vise à assurer que les outils d'enquête prévus par le droit national pour les affaires de criminalité organisée ou d'autres formes graves de criminalité puissent aussi servir dans les affaires de fraude et de contrefaçon des moyens de

paiement autres que les espèces, du moins dans les plus graves. Il doit aussi permettre qu'à la suite d'injonctions légales, des informations soient communiquées aux autorités sans retard indu.

*Article 13: Échange d'informations* — cet article devrait encourager à recourir davantage aux points de contact nationaux opérationnels.

*Article 14: Signalement des infractions* — cet article répond à la nécessité, soulignée dans l'analyse d'impact, d'augmenter et de faciliter les signalements d'infraction. Il vise à garantir l'existence de canaux de communication appropriés pour que les victimes et les entités privées puissent signaler les infractions et à encourager à effectuer les signalements sans retard indu, comme le fait une disposition similaire à l'article 16, paragraphe 2, de la directive 2011/93/UE relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie. Des exemples de mesures à prendre sont donnés au considérant 19.

*Article 15: Aide et soutien aux victimes* — cet article oblige les États membres à veiller à ce que les victimes de fraude aux moyens de paiement autres que les espèces disposent d'informations, de canaux de signalement des infractions et de conseils sur la façon de se protéger contre les conséquences négatives de la fraude et contre l'atteinte à leur réputation qui en découle.

Il s'applique aux personnes physiques et morales, qui sont également touchées par les conséquences des infractions visées par la proposition. Il introduit en outre des dispositions pour étendre aux personnes morales plusieurs droits spécifiques accordés aux personnes physiques par la directive 2012/29/UE.

*Article 16: Prévention* — cet article répond au besoin de sensibiliser le public et de réduire ainsi le risque de devenir une victime de la fraude, par des campagnes d'information et de sensibilisation, et des programmes de recherche et d'éducation. L'analyse d'impact a recensé les lacunes de la prévention parmi les sources du problème que constitue ce type de fraude. Cet article adopte une démarche similaire à celle de l'article 23 (Prévention) de la directive 2011/93/UE relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie.

*Article 17: Suivi et statistiques* — cet article répond au besoin d'établir des statistiques sur la fraude et la contrefaçon des moyens de paiement autres que les espèces, en obligeant les États membres à veiller à la mise en place d'un système adapté pour enregistrer, produire et fournir des statistiques sur les infractions visées dans la proposition de directive, et sur le suivi de l'efficacité de leurs systèmes (couvrant toutes les phases judiciaires) dans la lutte contre la fraude aux moyens de paiement autres que les espèces. Il adopte une démarche similaire à celle de l'article 14 (Suivi et statistiques) de la directive 2013/40/UE relative aux attaques contre les systèmes d'information, et de l'article 44 de la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme (4$^{e}$ directive antiblanchiment). Il doit aussi contribuer à remédier au manque actuel de données sur les fraudes, et aiderait ainsi à évaluer l'efficacité des systèmes nationaux dans la lutte contre la fraude aux moyens de paiement autres que les espèces.

*Article 18: Remplacement de la décision-cadre 2001/413/JAI* — cet article remplace les dispositions actuelles dans le domaine de la fraude et la contrefaçon des moyens de paiement autres que les espèces, pour les États membres participant à la présente directive.

*Articles 19, 20 et 21* — ces articles contiennent des dispositions supplémentaires relatives à la transposition par les États membres, à l'évaluation et aux rapports par la Commission et à l'entrée en vigueur de la directive.

2017/0226 (COD)

Proposition de

**DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL**

**concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces et remplaçant la décision-cadre 2001/413/JAI du Conseil**

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 83, paragraphe 1,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen,

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1) La fraude et la contrefaçon des moyens de paiement autres que les espèces constituent des menaces pour la sécurité car elles représentent une source de revenus pour la criminalité organisée et permettent ainsi à d'autres activités criminelles de se développer, comme le terrorisme, le trafic de stupéfiants et la traite des êtres humains.

(2) Elles font aussi obstacle au marché unique numérique, en sapant la confiance des consommateurs et en causant des préjudices économiques directs.

(3) La décision-cadre 2001/413/JAI[44] a besoin d'être actualisée et complétée par de nouvelles dispositions ayant trait aux infractions, aux sanctions et à la coopération transfrontière.

(4) L'existence de lacunes et de différences importantes dans les législations des États membres en matière fraude et de contrefaçon des moyens de paiement autres que les espèces risque d'entraver la lutte contre ce type d'infraction et d'autres infractions graves et organisées qui y sont liées et auxquelles il est propice, et de nuire à l'efficacité de la coopération policière et judiciaire dans ce domaine

(5) La fraude et la contrefaçon des moyens de paiement autres que les espèces ont une forte dimension transfrontière, accentuée par leur nature de plus en plus fréquemment

[44] Décision-cadre 2001/413/JAI du Conseil du 28 mai 2001 concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces (JO L 149 du 2.6.2001, p. 1).

numérique, qui souligne la nécessité d'œuvrer davantage à un rapprochement des législations pénales dans ce domaine.

(6) Ces dernières années, on a assisté non seulement à un essor exponentiel de l'économie numérique mais aussi à une prolifération de l'innovation dans maints secteurs, dont celui des technologies de paiement. Ces technologies novatrices impliquent l'utilisation de nouveaux instruments de paiement qui, tout en créant des opportunités nouvelles pour les consommateurs et les entreprises, augmentent aussi les possibilités de fraude. Le cadre juridique doit par conséquent rester pertinent et à jour dans ce contexte d'évolution technologique.

(7) Il importe d'adopter des définitions communes dans ce domaine pour garantir une approche cohérente des États membres quant à l'application de la présente directive. Les définitions doivent englober de nouveaux types d'instruments de paiement, comme l'argent électronique et les monnaies virtuelles.

(8) Protéger par le droit pénal, en priorité, les instruments de paiement qui sont dotés d'une forme spéciale de protection contre l'imitation ou la fraude a pour but d'encourager les opérateurs à prévoir ces formes spéciales de protection pour les instruments de paiement qu'ils émettent, et d'ajouter ainsi à l'instrument un élément de prévention.

(9) Des mesures de droit pénal effectives et efficaces sont indispensables pour protéger les moyens de paiement autres que les espèces de la fraude et de la contrefaçon. Il est plus particulièrement nécessaire de traiter de la même façon, en droit pénal, les éléments constitutifs des agissements délictueux qui contribuent à l'utilisation frauduleuse des moyens de paiement ou lui ouvrent la voie. Des agissements tels que la collecte et la possession d'instruments de paiement dans l'intention de commettre une fraude, au moyen, par exemple, de l'hameçonnage ou de la copie, et leur diffusion, par exemple en vendant des informations relatives à des cartes de crédit sur l'internet, devraient dès lors être incriminés à part entière, sans être directement liés à l'utilisation frauduleuse de moyens de paiement. Ainsi, ces agissements délictueux devraient aussi inclure les cas où la possession, l'obtention ou la diffusion ne conduit pas nécessairement à l'utilisation frauduleuse de ces instruments de paiement, lorsque l'auteur de l'infraction a connaissance d'une telle possibilité (*dolus eventualis*). La présente directive ne sanctionne pas l'utilisation légitime d'un instrument de paiement, notamment dans le cadre de la prestation de services de paiement innovants, comme ceux généralement mis au point par les sociétés de technologie financière.

(10) Les sanctions et peines infligées pour fraude et contrefaçon des moyens de paiement autres que les espèces devraient être effectives, proportionnées et dissuasives dans toute l'Union.

(11) Il est justifié de prévoir des peines plus sévères lorsque des infractions sont commises par une organisation criminelle, au sens de la décision-cadre 2008/841/JAI du Conseil[45], ou lorsqu'elles sont commises à grande échelle et causent ainsi un préjudice grave ou considérable aux victimes ou procurent à leur auteur un avantage cumulé égal à au moins 20 000 EUR.

[45] Décision-cadre 2008/841/JAI du Conseil du 24 octobre 2008 relative à la lutte contre la criminalité organisée (JO L 300 du 11.11.2008, p. 42).

(12) Les règles juridictionnelles devraient garantir que les infractions visées dans la présente directive fassent l'objet de poursuites effectives et efficaces. En général, c'est le système de justice pénale du pays dans lequel une infraction a lieu qui est le plus à même de la traiter. Les États membres devraient donc établir leur compétence juridictionnelle à l'égard des infractions commises sur leur territoire, de celles commises par leurs ressortissants et de celles qui causent un préjudice sur leur territoire.

(13) Les systèmes d'information remettent en cause la notion traditionnelle de territorialité parce qu'en principe, ils peuvent être utilisés et contrôlés à distance à partir de n'importe où. Lorsque les États membres établissent leur compétence sur le fondement de la commission des infractions sur leur territoire, il apparaît judicieux d'examiner également la portée de leur compétence en ce qui concerne les infractions commises à l'aide de systèmes d'information. Dans de tels cas, un État membre devrait avoir compétence lorsque le système d'information est situé sur son territoire alors que l'auteur de l'infraction ne s'y trouve pas, et lorsque l'auteur se trouve sur le territoire de l'État membre alors que le système d'information est situé en dehors de celui-ci.

(14) Il doit être remédié à la complexité que revêt l'attribution de la compétence lorsque les effets d'une infraction se produisent dans un pays autre que celui dans lequel cette dernière a été commise. La compétence à l'égard des infractions devrait dès lors être établie en tenant compte non pas de la nationalité et de la présence physique de leur auteur, mais de tout préjudice causé par ces agissements sur le territoire de l'État membre.

(15) Des outils spéciaux étant nécessaires pour mener efficacement les enquêtes sur la fraude et la contrefaçon des moyens de paiement autres que les espèces, et ces outils étant propices à une bonne coopération internationale entre les autorités nationales, les autorités compétentes de tous les États membres devraient avoir accès, pour les enquêtes sur ce type d'infraction, aux outils d'enquête généralement utilisés pour les affaires de criminalité organisée ou concernant d'autres infractions graves. Eu égard au principe de proportionnalité, le recours à ces outils conformément au droit national devrait être proportionné à la nature et à la gravité des infractions sous enquête. En outre, les services répressifs et les autres autorités compétentes devraient avoir accès, au moment où ils en ont besoin, aux informations qui leur sont utiles pour mener les enquêtes et exercer les poursuites à l'encontre des infractions visées dans la présente directive.

(16) Dans nombre de cas, des activités criminelles sont à l'origine d'incidents qui devraient être signalés aux autorités nationales compétentes, en application de la directive (UE) 2016/1148 du Parlement européen et du Conseil[46]. La nature criminelle de tels incidents peut être soupçonnée même lorsqu'il n'existe pas de preuve manifeste d'une infraction pénale dès le départ. Aussi les opérateurs de services essentiels et les fournisseurs de service numérique devraient-ils être encouragés à communiquer aux services répressifs les rapports requis par la directive (EU) 2016/1148, de façon à permettre une action efficace et globale et à faciliter l'imputation des infractions et la reconnaissance de ces actes par leurs auteurs. On ne saurait favoriser un

[46] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194 du 19.7.2016, p. 1).

environnement sûr, sécurisé et plus résilient sans un signalement systématique aux services répressifs des incidents susceptibles de constituer des infractions pénales graves. En outre, lorsque c'est utile, les centres de réponse aux incidents de sécurité informatiques désignés conformément à l'article 9 de la directive (UE) 2016/1148 devraient participer aux enquêtes des services répressifs afin de fournir des informations, si les autorités nationales le jugent opportun, et d'apporter leur expertise en matière de systèmes d'information.

(17) Les incidents de sécurité majeurs, au sens de l'article 96 de la directive (UE) 2015/2366 du Parlement européen et du Conseil[47], peuvent être d'origine criminelle. Lorsque c'est utile, les prestataires de services de paiement devraient être encouragés à communiquer aux services répressifs les rapports que la directive (UE) 2015/2366 les oblige à présenter à l'autorité compétente de leur État membre.

(18) Plusieurs instruments et mécanismes existent au niveau de l'Union pour permettre l'échange d'informations entre les services répressifs nationaux dans le cadre des enquêtes et des poursuites. Afin de faciliter et d'accélérer la coopération entre les services répressifs nationaux et de garantir que ces instruments et mécanismes soient exploités au mieux, la présente directive devrait accroître le rôle des points de contact opérationnels créés par la décision-cadre 2001/413/JAI du Conseil. Les États membres peuvent décider de recourir au réseau existant de ces points de contact, tel que celui visé dans la directive 2013/40/UE du Parlement européen et du Conseil[48]. Ils devraient apporter une aide effective, par exemple en facilitant l'échange d'informations utiles et en apportant des conseils techniques ou des informations juridiques. Pour que le réseau fonctionne bien, chaque point de contact devrait être en mesure de communiquer rapidement avec son homologue d'un autre État membre. Eu égard à la forte dimension transfrontière de ce domaine de la criminalité et, en particulier, à la nature volatile des preuves électroniques, les États membres devraient pouvoir traiter promptement les demandes urgentes reçues de ce réseau de points de contact et donner une réponse dans un délai de huit heures.

(19) Signaler sans retard indu les infractions aux autorités publiques est essentiel à la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces, car c'est fréquemment le point de départ de l'enquête judiciaire. Il convient donc d'adopter des mesures pour encourager les personnes physiques et morales, en particulier les établissements financiers, à signaler les infractions aux services répressifs et aux autorités judiciaires. Ces mesures peuvent être instaurées par diverses formes d'action, y compris législative, par exemple l'obligation de signaler les soupçons de fraude, ou non législative, comme la création ou le financement d'organisations ou de mécanismes favorisant l'échange d'informations, ou des campagnes de sensibilisation. Toute mesure qui implique le traitement de données à caractère personnel relatives à des personnes physiques doit être mise en œuvre dans

---

47 Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE, 2013/36/UE et le règlement (UE) no 1093/2010, et abrogeant la directive 2007/64/CE (JO L 337 du 23.12.2015, p. 35).

48 Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil (JO L 218 du 14.8.2013, p. 8).

le respect du règlement (UE) 2016/679 du Parlement européen et du Conseil[49]. En particulier, toute transmission d'informations concernant la prévention et la répression des infractions liées à la fraude et à la contrefaçon des moyens de paiement autres que les espèces doit respecter les exigences fixées dans le règlement (UE) 2016/679, notamment les motifs licites du traitement.

(20) La fraude et la contrefaçon des moyens de paiement autres que les espèces peuvent avoir de graves conséquences économiques et non économiques pour leurs victimes. Lorsque ce type de fraude comprend une usurpation d'identité, ses conséquences en sont souvent aggravées, à cause de l'atteinte à la réputation et du grave dommage émotionnel. Il convient que les États membres adoptent des mesures d'aide, de soutien et de protection destinées à atténuer ces conséquences.

(21) Les personnes physiques victimes d'une fraude relative aux moyens de paiement autres que les espèces jouissent de droits conférés par la directive 2012/29/UE du Parlement européen et du Conseil[50]. Les États membres devraient adopter des mesures d'aide et de soutien à ces victimes qui soient inspirées des mesures requises par cette directive 2012/29/UE mais répondent plus directement aux besoins spécifiques des victimes d'une fraude liée à une usurpation d'identité. Il devrait s'agir, notamment, d'un soutien psychologique spécialisé et de conseils financiers, pratiques et juridiques, ainsi que d'une assistance pour obtenir les indemnisations prévues pour ces cas. Les personnes physiques devraient aussi bénéficier d'informations et de conseils sur la façon de se protéger contre les conséquences négatives de ce type d'infraction.

(22) La présente directive devrait prévoir, pour les personnes morales, le droit d'obtenir des informations sur les procédures de dépôt de plainte. Ce droit est plus particulièrement nécessaire aux petites et moyennes entreprises[51] et devrait permettre de créer un environnement correspondant mieux à leurs besoins. Les personnes physiques bénéficient déjà de ce droit en vertu de la directive 2012/29/UE.

(23) Les États membres devraient adopter ou renforcer un ensemble de mesures destinées à prévenir la fraude et la contrefaçon des moyens de paiement autres que les espèces, et des initiatives visant à réduire le risque de devenir victime de telles infractions, par des campagnes d'information et de sensibilisation et des programmes de recherche et d'éducation.

(24) Il est nécessaire de collecter des données comparables sur les infractions visées dans la présente directive. Les données pertinentes devraient être mises à la disposition des agences et organes spécialisés compétents de l'Union, tels qu'Europol, en fonction de leur mission et de leurs besoins d'informations. L'objectif serait de dresser un tableau plus complet de la fraude et la contrefaçon des moyens de paiement autres que les espèces, ainsi que des problèmes que pose la sécurité des paiements au niveau de

---

[49] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

[50] Directive 2012/29/UE du Parlement européen et du Conseil du 25 octobre 2012 établissant des normes minimales concernant les droits, le soutien et la protection des victimes de la criminalité et remplaçant la décision-cadre 2001/220/JAI du Conseil (JO L 315 du 14.11.2012, p. 57).

[51] Recommandation de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises (JO L 124 du 20.5.2003, p. 36).

l'Union, et de contribuer à l'élaboration d'une action plus efficace pour y remédier. Les États membres devraient tirer tout le parti possible des pouvoirs d'Europol et de sa capacité à apporter une aide et un soutien dans les enquêtes en ces matières, en lui communiquant des informations sur les modes opératoires des fraudeurs pour qu'il puisse procéder à des analyses stratégiques et à des évaluations de la menace que posent la fraude et la contrefaçon des moyens de paiement autres que les espèces, conformément au règlement (UE) 2016/794 du Parlement européen et du Conseil[52]. Ces informations transmises peuvent permettre de mieux comprendre les menaces présentes et futures et aider le Conseil et la Commission à établir les priorités stratégiques et opérationnelles de l'Union aux fins de la lutte contre la criminalité, ainsi que les modalités de mise en œuvre de ces priorités.

(25) La présente directive vise à modifier et à étendre les dispositions de la décision-cadre 2001/413/JAI du Conseil. Les modifications à apporter étant significatives par leur nombre comme par leur nature, il convient, pour plus de clarté, de remplacer entièrement la décision-cadre 2001/413/JAI pour les États membres liés par la présente directive.

(26) Conformément à l'article 3 du protocole n° 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, ces États membres ont notifié leur souhait de participer à l'adoption et à l'application de la présente directive.

OU

(26) Conformément à l'article 3 du protocole nº 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Royaume-Uni a notifié [, par lettre du...,] son souhait de participer à l'adoption et à l'application de la présente directive.

OU

(26) Conformément à l'article 3 du protocole nº 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, l'Irlande a notifié [, par lettre du...,] son souhait de participer à l'adoption et à l'application de la présente directive.

ET/OU

(26) Conformément aux articles 1er et 2 du protocole n° 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, et sans préjudice de l'article 4 dudit protocole, ces États membres ne participent pas à

[52] Règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI (JO L 135 du 24.5.2016, p. 53).

l'adoption de la présente directive et ne sont donc pas liés par celle-ci ni soumis à son application.

OU

(26) Conformément aux articles 1er et 2 du protocole nº 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, et sans préjudice de l'article 4 dudit protocole, l'Irlande ne participe pas à l'adoption de la présente directive et n'est pas liée par celle-ci ni soumise à son application.

OU

(26) Conformément aux articles 1er et 2 du protocole n° 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, et sans préjudice de l'article 4 dudit protocole, le Royaume-Uni ne participe pas à l'adoption de la présente directive et n'est pas lié par celle-ci ni soumis à son application.

(27) Conformément aux articles 1er et 2 du protocole n° 22 sur la position du Danemark annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Danemark ne participe pas à l'adoption de la présente directive et n'est pas lié par celle-ci ni soumis à son application.

(28) Étant donné que les objectifs de la présente directive, à savoir rendre la fraude et la contrefaçon des moyens de paiement autres que les espèces passibles de sanctions pénales effectives, proportionnées et dissuasives, et améliorer et favoriser la coopération judiciaire, entre les autorités compétentes, d'une part, et entre les personnes physiques et morales et les autorités compétentes, d'autre part, ne peuvent être atteints de manière suffisante par les États membres et peuvent donc, en raison de leurs dimensions ou de leurs effets, être mieux atteints au niveau de l'Union, celle-ci peut prendre des mesures conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité tel qu'énoncé audit article, la présente directive n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

(29) La présente directive respecte les droits fondamentaux et observe les principes reconnus, en particulier, par la charte des droits fondamentaux de l'Union européenne, notamment le droit à la liberté et à la sûreté, le respect de la vie privée et familiale, la protection des données à caractère personnel, la liberté d'entreprise, le droit de propriété, le droit à un recours effectif et à accéder à un tribunal impartial, la présomption d'innocence et les droits de la défense, les principes de légalité et de proportionnalité des délits et des peines, ainsi que le droit à ne pas être jugé ou puni pénalement deux fois pour une même infraction. La présente directive cherche en particulier à garantir le respect absolu de ces droits et principes et devrait être mise en œuvre en conséquence,

ONT ADOPTÉ LA PRÉSENTE DIRECTIVE:

# TITRE I: OBJET ET DÉFINITIONS

*Article premier*
*Objectif*

La présente directive établit des règles minimales relatives à la définition des infractions pénales et des sanctions en matière de fraude et de contrefaçon des moyens de paiement autres que les espèces.

*Article 2*
*Définitions*

Aux fins de la présente directive, on entend par:

(a) «instrument de paiement»: un dispositif, objet ou enregistrement protégé, autre que la monnaie légale, qui, à lui seul ou avec une procédure ou un ensemble de procédures, permet à son titulaire ou son utilisateur d'effectuer un transfert d'argent ou de valeur monétaire ou d'initier un ordre de paiement, y compris au moyen d'instruments d'échange numériques;

(b) «dispositif, objet ou enregistrement protégé»: un dispositif, objet ou enregistrement protégé contre les imitations et les utilisations frauduleuses, par exemple dans sa conception ou par un codage ou une signature;

(c) «ordre de paiement»: un ordre de paiement au sens de l'article 4, point 13), de la directive (UE) 2015/2366;

(d) «instrument d'échange numérique»: toute monnaie électronique au sens de l'article 2, point 2), de la directive 2009/110/CE du Parlement européen et du Conseil[53], et les monnaies virtuelles;

(e) «monnaies virtuelles»: une représentation numérique de valeur qui n'est ni émise par une banque centrale ou une autorité publique, ni nécessairement attachée à une monnaie à cours forcé, mais est acceptée comme moyen de paiement par des personnes physiques ou morales et peut être transférée, stockée, ou échangée par voie électronique;

(f) «service de paiement»: un service de paiement au sens de l'article 4, point 3), de la directive (UE) 2015/2366;

[53] Directive 2009/110/CE du Parlement européen et du Conseil du 16 septembre 2009 concernant l'accès à l'activité des établissements de monnaie électronique et son exercice ainsi que la surveillance prudentielle de ces établissements, modifiant les directives 2005/60/CE et 2006/48/CE et abrogeant la directive 2000/46/CE (JO L 267 du 10.10.2009, p. 7).

(g) «utilisateur de services de paiement»: un utilisateur de services de paiement au sens de l'article 4, point 10), de la directive (UE) 2015/2366;

(h) «compte de paiement»: un compte de paiement au sens de l'article 4, point 12), de la directive (UE) 2015/2366;

(i) «opération de paiement»: une opération de paiement au sens de l'article 4, point 5), de la directive (UE) 2015/2366;

(j) «payeur»: une personne physique ou morale qui est titulaire d'un compte de paiement et autorise un ordre de paiement à partir de ce compte de paiement, ou, en l'absence de compte de paiement, une personne physique ou morale qui donne un ordre de paiement ou transfère une monnaie virtuelle;

(k) «bénéficiaire»: un bénéficiaire au sens de l'article 4, point 9), de la directive (UE) 2015/2366;

(l) «système d'information»: un système d'information au sens de l'article 2, point a), de la directive 2013/40/UE;

(m) «données informatiques»: des données informatiques au sens de l'article 2, point b), de la directive 2013/40/UE.

## TITRE II: INFRACTIONS

*Article 3*
*Utilisation frauduleuse des instruments de paiement*

Les États membres prennent les mesures nécessaires pour ériger en infractions pénales punissables les agissements suivants, lorsqu'ils sont intentionnels:

(a) l'utilisation frauduleuse d'un instrument de paiement volé ou obtenu par d'autres moyens illégaux;

*(b)* l'utilisation frauduleuse d'un instrument de paiement faux ou falsifié;

*Article 4*
*Infractions préparatoires à l'utilisation frauduleuse d'instruments de paiement*

Les États membres prennent les mesures nécessaires pour ériger en infractions pénales punissables les agissements suivants, lorsqu'ils sont intentionnels:

(a) le vol ou autre appropriation illégale d'un instrument de paiement;

(b) la contrefaçon ou la falsification d'un instrument de paiement en vue de son utilisation frauduleuse;

(c) la possession, l'obtention aux fins d'utilisation, l'importation, l'exportation, la vente, le transport, la diffusion ou toute autre forme de mise à disposition d'un instrument

de paiement volé ou obtenu par d'autres moyens illégaux, ou faux ou falsifié, en vue de son utilisation frauduleuse.

*Article 5*
*Infractions liées aux systèmes d'information*

Les États membres prennent les mesures nécessaires pour ériger en infraction pénale punissable, lorsqu'il est intentionnel, le fait d'effectuer ou de faire effectuer un transfert d'argent, de valeur monétaire ou de monnaies virtuelles, dans le but de procurer un gain illégal à l'auteur de l'infraction ou à un tiers, en:

(a) empêchant ou perturbant le fonctionnement d'un système informatique;

(b) introduisant, altérant, effaçant, transmettant ou supprimant des données informatiques.

*Article 6*
*Outils utilisés pour commettre les infractions*

Les États membres prennent les mesures nécessaires pour ériger en infractions pénales punissables, lorsqu'ils sont intentionnels, la production, l'obtention aux fins d'utilisation, l'importation, l'exportation, la vente, le transport, la diffusion ou toute autre forme de mise à disposition d'un dispositif ou d'un instrument, de données informatiques ou d'autres moyens spécialement conçus ou adaptés pour commettre l'une des infractions visées à l'article 4, points a) et b), ou à l'article 5.

*Article 7*
*Instigation, complicité et tentative*

1. Les États membres prennent les mesures nécessaires pour ériger en infraction pénale punissable l'instigation d'une infraction visée aux articles 3 à 6 ou le fait de s'en rendre complice.

2. Les États membres prennent les mesures nécessaires pour ériger en infraction pénale punissable la tentative de commettre une infraction visée aux articles 3 à 6.

*Article 8*
*Sanctions à l'encontre des personnes physiques*

1. Les États membres prennent les mesures nécessaires pour que les infractions visées aux articles 3 à 7 soient passibles de sanctions pénales effectives, proportionnées et dissuasives.

2. Les États membres prennent les mesures nécessaires pour que les infractions visées aux articles 3, 4 et 5 soient passibles d'une peine d'emprisonnement maximale d'au moins trois ans.

3. Les États membres prennent les mesures nécessaires pour que les infractions visées à l'article 6 soient passibles d'une peine d'emprisonnement maximale d'au moins deux ans.

4. Les États membres prennent les mesures nécessaires pour que les infractions visées aux articles 3, 4 et 5 soient passibles d'une peine d'emprisonnement maximale d'au moins cinq ans dans le cas où:

(a) elles sont commises dans le cadre d'une organisation criminelle au sens de la décision-cadre 2008/841/JAI, indépendamment de la sanction qui y est prévue;

(b) elles causent un préjudice grave ou considérable ou procurent un avantage cumulé égal à au moins 20 000 EUR.

*Article 9*
*Responsabilité des personnes morales*

1. Les États membres prennent les mesures nécessaires pour que les personnes morales puissent être tenues pour responsables des infractions visées aux articles 3 à 7, commises pour leur compte par toute personne, agissant individuellement ou en qualité de membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé sur:

(a) un pouvoir de représentation de la personne morale;

(b) un pouvoir de prendre des décisions au nom de la personne morale;

(c) un pouvoir d'exercer un contrôle au sein de la personne morale.

2. Les États membres prennent les mesures nécessaires pour que les personnes morales puissent être tenues pour responsables lorsque le défaut de surveillance ou de contrôle de la part d'une personne visée au paragraphe 1 a rendu possible la commission de l'une des infractions visées aux articles 3 à 7 pour le compte de ladite personne morale, par une personne soumise à son autorité.

3. La responsabilité des personnes morales au titre des paragraphes 1 et 2 n'exclut pas les poursuites pénales contre les personnes physiques auteurs, instigatrices ou complices de l'une des infractions visées aux articles 3 à 7.

*Article 10*
*Sanctions à l'encontre des personnes morales*

Les États membres prennent les mesures nécessaires pour qu'une personne morale déclarée responsable au titre de l'article 9, paragraphe 1, soit passible de sanctions effectives, proportionnées et dissuasives, qui incluent des amendes pénales ou non pénales, et éventuellement d'autres sanctions, telles que:

(a) l'exclusion du bénéfice d'un avantage ou d'une aide publics;

(b) l'interdiction temporaire ou définitive d'exercer une activité commerciale;

(c) le placement sous surveillance judiciaire;

(d) une mesure judiciaire de dissolution;

(e) la fermeture temporaire ou définitive d'établissements ayant servi à commettre l'infraction.

## TITRE III: COMPÉTENCE JURIDICTIONNELLE ET ENQUÊTES

*Article 11*
*Compétence juridictionnelle*

1. Chaque État membre prend les mesures nécessaires pour établir sa compétence à l'égard des infractions visées aux articles 3 à 7 lorsque:

   (a) l'infraction a été commise, en tout ou en partie, sur son territoire;

   (b) l'auteur de l'infraction est l'un de ses ressortissants;

   (c) l'infraction a causé un préjudice sur son territoire, y compris un préjudice résultant de l'usurpation de l'identité d'une personne.

2. Lorsqu'il établit sa compétence conformément au paragraphe 1, point a), un État membre veille à être compétent lorsque:

   (a) l'auteur de l'infraction a commis celle-ci alors qu'il était physiquement présent sur son territoire, que les ordinateurs ou le système d'information utilisés à cet effet soient situés sur son territoire ou non;

   (b) l'infraction a été commise à l'aide d'ordinateurs ou d'un système d'information situés sur son territoire, que l'auteur de l'infraction soit physiquement présent sur son territoire ou non lors de la commission de l'infraction.

3. Un État membre informe la Commission de sa décision d'établir sa compétence à l'égard d'une infraction visée aux articles 3 à 7 qui a été commise en dehors de son territoire, notamment dans les cas suivants:

   (a) l'auteur de l'infraction réside habituellement sur son territoire;

   (b) l'infraction a été commise pour le compte d'une personne morale établie sur son territoire;

   (c) l'infraction a été commise à l'encontre de l'un de ses ressortissants ou d'une personne résidant habituellement sur son territoire.

*Article 12*
*Efficacité des enquêtes*

1. Les États membres prennent les mesures nécessaires pour que des outils d'enquête efficaces, tels que ceux qui sont utilisés dans les affaires de criminalité organisée ou d'autres formes graves de criminalité, soient mis à la disposition des personnes, des unités ou des services chargés des enquêtes ou des poursuites concernant les infractions visées aux articles 3 à 7.

2. Les États membres prennent les mesures nécessaires pour que, lorsque le droit national oblige des personnes physiques et morales à communiquer des informations relatives aux infractions visées aux articles 3 à 7, les autorités chargées des enquêtes ou des poursuites concernant ces infractions reçoivent lesdites informations sans retard indu.

# TITRE IV: ÉCHANGE D'INFORMATIONS ET SIGNALEMENT DES INFRACTIONS

*Article 13*
*Échange d'informations*

1. Aux fins de l'échange d'informations relatives aux infractions visées aux articles 3 à 7, les États membres veillent à disposer d'un point de contact national opérationnel, disponible vingt-quatre heures sur vingt-quatre et sept jours sur sept. Ils veillent également à mettre des procédures en place pour traiter rapidement les demandes urgentes d'assistance et pour que l'autorité compétente réponde dans un délai de huit heures à compter de la réception de la demande, en indiquant au moins si la demande sera satisfaite et la forme et le délai estimé pour cette réponse Les États membres peuvent décider de recourir aux réseaux existants de points de contact opérationnels.

2. Les États membres communiquent à la Commission, à Europol et à Eurojust le point de contact visé au paragraphe 1 qu'ils ont désigné. La Commission transmet ces informations aux autres États membres.

*Article 14*
*Signalement des infractions*

1. Les États membres prennent les mesures nécessaires pour que des canaux de communication appropriés soient mis à disposition afin de faciliter le signalement aux services répressifs et aux autres autorités nationales compétentes, sans retard indu, des infractions visées aux articles 3 à 7.

2. Les États membres prennent les mesures nécessaires pour encourager les établissements financiers et les autres personnes morales exerçant une activité sur leur territoire à signaler, sans retard indu, les soupçons de fraude aux services répressifs et aux autres autorités compétentes, aux fins de la détection et de la prévention des infractions visées aux articles 3 à 7 et des enquêtes et poursuites les concernant.

## TITRE V: AIDE AUX VICTIMES ET PRÉVENTION

*Article 15*
*Aide et soutien aux victimes*

1. Les États membres veillent à ce que les personnes physiques et morales qui ont subi un préjudice à la suite d'infractions visées aux articles 3 à 7, commises par l'utilisation abusive de données à caractère personnel, bénéficient d'informations et de conseils sur la façon de se protéger contre les conséquences négatives de ces infractions, telles que l'atteinte à la réputation.

2. Les États membres veillent à ce que les personnes morales victimes d'infractions visées aux articles 3 to 7 de la présente directive bénéficient, sans retard indu après leur premier contact avec une autorité compétente, d'informations sur:

   (a) les procédures de dépôt de plainte concernant l'infraction et le rôle de la victime dans ces procédures;

   (b) les procédures disponibles pour introduire une réclamation si l'autorité compétente ne respecte pas leurs droits au cours de la procédure pénale;

   (c) les coordonnées utiles pour l'envoi de communications relatives à leur dossier;

*Article 16*
*Prévention*

Les États membres prennent des mesures appropriées, y compris sur l'internet, telles que des campagnes d'information et de sensibilisation, des programmes de recherche et d'éducation, en coopération avec des parties prenantes s'il y a lieu, pour réduire la fraude en général, sensibiliser le public et réduire le risque que des personnes deviennent victimes d'une fraude.

## TITRE VI: DISPOSITIONS FINALES

*Article 17*
*Suivi et statistiques*

1. Au plus tard [3 mois après l'entrée en vigueur de la présente directive], la Commission établit un programme détaillé de suivi des réalisations, résultats et effets de la présente directive. Le programme de suivi définit les moyens à utiliser et les intervalles à appliquer pour recueillir les données et autres éléments de preuves nécessaires. Il précise les rôles respectifs de la Commission et des États membres dans la collecte, le partage et l'analyse des données et des autres éléments de preuve.

2. Les États membres veillent à mettre en place un système d'enregistrement, de production et de communication de statistiques mesurant les phases de signalement, d'enquête et de procès relatives aux infractions visées aux articles 3 à 7.

3. Les statistiques visées au paragraphe 2 portent, au minimum, sur le nombre d'infractions visées aux articles 3 à 7 qui ont été signalées aux États membres, le nombre d'enquêtes ouvertes, le nombre de personnes poursuivies et condamnées pour lesdites infractions et le fonctionnement des phases de signalement, d'enquête et de procès relatives à ces infractions.

4. Les États membres transmettent chaque année à la Commission les données recueillies conformément aux paragraphes 1, 2 et 3. La Commission veille à ce qu'un état consolidé des rapports statistiques soit publié chaque année et soumis aux agences et organes spécialisés compétents de l'Union.

*Article 18*
*Remplacement de la décision-cadre 2001/413/JAI*

La décision-cadre 2001/413/JAI est remplacée en ce qui concerne les États membres liés par la présente directive, sans préjudice des obligations de ces États membres concernant le délai de transposition de ladite décision-cadre en droit interne.

En ce qui concerne les États membres liés par la présente directive, les références faites à la décision-cadre 2001/413/JAI s'entendent comme faites à la présente directive.

*Article 19*
*Transposition*

1. Les États membres mettent en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive au plus tard [24 mois après l'entrée en vigueur]. Ils en informent immédiatement la Commission.

2. Lorsque les États membres adoptent ces dispositions, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication officielle. Les modalités de cette référence sont arrêtées par les États membres.

3. Les États membres communiquent à la Commission le texte des mesures qu'ils adoptent dans le domaine régi par la présente directive.

*Article 20*
*Évaluation et rapport*

1. La Commission présente au Parlement européen et au Conseil, au plus tard [48 mois après l'entrée en vigueur], un rapport évaluant dans quelle mesure les États membres ont pris les mesures nécessaires pour se conformer à la présente directive. Les États membres fournissent à la Commission les informations nécessaires à l'établissement du rapport.

2. La Commission procède, au plus tard [96 mois après l'entrée en vigueur], à une évaluation de la présente directive relative à la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces et remet un rapport au Parlement européen et au Conseil.

*Article 21*
*Entrée en vigueur*

La présente directive entre en vigueur le vingtième jour suivant celui de sa publication au Journal officiel de l'Union européenne.

Les États membres sont destinataires de la présente directive conformément aux traités.

Fait à Bruxelles, le

| | |
|---|---|
| *Par le Parlement européen* | *Par le Conseil* |
| *Le président* | *Le président* |