Conseil de
l'Union européenne

Bruxelles, le 11 juillet 2023
(OR. en)

11761/23

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

NOTE DE TRANSMISSION

Origine:	Pour la secrétaire générale de la Commission européenne, Madame Martine DEPREZ, directrice
Date de réception:	10 juillet 2023
Destinataire:	Madame Thérèse BLANCHET, secrétaire générale du Conseil de l'Union européenne
N° doc. Cion:	COM(2023) 363 final
Objet:	RAPPORT DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL évaluant dans quelle mesure les États membres ont pris les mesures nécessaires pour se conformer à la directive (UE) 2019/713 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(2023) 363 final.

p.j.: COM(2023) 363 final

COMMISSION
EUROPÉENNE

Bruxelles, le 10.7.2023
COM(2023) 363 final

RAPPORT DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

évaluant dans quelle mesure les États membres ont pris les mesures nécessaires pour se conformer à la directive (UE) 2019/713 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

1. Introduction

La fraude et la contrefaçon des moyens de paiement autres que les espèces, tels que les cartes de crédit ou de paiement, représentent une source de revenus pour la criminalité organisée et permettent à d'autres activités criminelles de se développer, comme le terrorisme, le trafic de stupéfiants et la traite des êtres humains. Ces infractions sont à l'origine de pertes importantes: la valeur totale des opérations frauduleuses commises à l'aide de cartes émises au sein de l'espace unique de paiements en euros (SEPA) s'élevait à 1,87 milliard d'EUR en 2019[1]. La grande majorité des opérations frauduleuses sont liées à des fraudes sans présence de la carte: en 2019, 80 % de la valeur des fraudes à la carte résultaient de fraudes sans présence de la carte, c'est-à-dire des paiements par l'internet, courrier électronique ou téléphone[2]. En 2019, le préjudice causé par les fraudes sans présence de la carte s'élevait à 1,50 milliard d'EUR, soit une progression de 4,3 % par rapport à l'année précédente[3].

La dimension transfrontière est manifeste: en 2019, plus de la moitié de la valeur totale des fraudes commises était liée à des transactions transfrontières au sein du SEPA. D'un point de vue géographique, en 2019, les transactions nationales représentaient 89 % de la valeur totale des transactions par carte, mais seulement 35 % de la valeur des opérations frauduleuses. Les transactions transfrontières au sein du SEPA représentaient 9 % de la valeur totale des transactions par carte, mais 51 % des fraudes signalées[4].

Afin de lutter de manière efficace contre ces infractions, les États membres doivent parvenir à une définition commune de ce qui devrait être considéré comme constituant la fraude et la contrefaçon des moyens de paiement autres que les espèces. Ils doivent également harmoniser leurs niveaux de sanctions et les moyens opérationnels consacrés au signalement des infractions et à l'échange d'informations entre les autorités. En conséquence, le 17 avril 2019, le Parlement européen et le Conseil ont adopté la directive (UE) 2019/713 (ci-après la "directive") 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[5]. Le présent rapport satisfait à l'exigence visée à l'article 21 de la directive.

1.1. Objectifs et champ d'application de la directive

La directive a pour objectif de rapprocher les droits pénaux des États membres[6] en matière de fraude et de contrefaçon des moyens de paiement autres que les espèces et d'améliorer la coopération entre les autorités compétentes. À cette fin, la directive établit des règles minimales relatives à la définition des infractions pénales et des sanctions. Le champ d'application de la directive est vaste, puisqu'il englobe tout "dispositif, objet ou

[1] Banque centrale européenne, "Seventh report on card fraud", disponible à l'adresse suivante: https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202110~cac4c418e8.en.html

[2] Ibidem.

[3] Ibidem.

[4] Ibidem.

[5] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv:OJ.L_.2019.123.01.0018.01.FRA.

[6] Dans la suite du présent rapport et sauf indication contraire, le terme "États membres" ou "tous les États membres" fait référence aux États membres liés par la directive, c'est-à-dire à tous les États membres de l'Union européenne à l'exception du Danemark et de l'Irlande, qui n'ont pas participé à l'adoption de la directive, conformément au protocole sur la position du Danemark annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne (TFUE), et conformément au protocole nº 21 sur la position du Royaume-Uni et de l'Irlande, respectivement.

enregistrement protégé non matériel ou matériel ou une combinaison de ces éléments, autre que la monnaie légale, qui, à lui seul ou en liaison avec une procédure ou un ensemble de procédures, permet à son titulaire ou à son utilisateur d'effectuer un transfert d'argent ou de valeur monétaire, y compris par des moyens d'échange numériques" [article 2, point a)[7]]. Par exemple, une application de paiement mobile en liaison avec une procédure d'autorisation (par exemple, un code PIN) serait visée par cette définition. Les monnaies virtuelles relèvent également du champ d'application de la directive [article 2, point d), et article 6].

La directive définit des infractions pénales spécifiques, à savoir:

- utilisation frauduleuse des instruments de paiement autres que les espèces (article 3);
- infractions liées à l'utilisation frauduleuse d'instruments de paiement matériels autres que les espèces (article 4);
- infractions liées à l'utilisation frauduleuse d'instruments de paiement non matériels autres que les espèces (article 5);
- fraude liée aux systèmes d'information (article 6);
- fourniture illégale d'outils utilisés pour commettre les infractions susmentionnées (article 7).

De plus, la directive **étend la responsabilité pénale** à l'instigation, par des personnes physiques ou morales, à commettre les infractions susmentionnées, au fait de s'en rendre complice et à la tentative de les commettre (article 8).

L'article 9 prévoit le niveau minimal des **sanctions** maximales pour les infractions mentionnées dans la directive.

Les articles suivants établissent les conditions minimales de la **responsabilité des personnes morales** (article 10) et des sanctions à leur encontre, qui incluent des amendes pénales ou non pénales, et fournissent une liste indicative des autres sanctions qui peuvent leur être appliquées (article 11).

L'article 12 a pour objectif de faire en sorte que les auteurs d'infractions, tels qu'ils sont définis dans la directive, soient poursuivis pour les infractions visées aux articles 3 à 8 de la directive. La **compétence** d'un État membre doit être établie si a) l'infraction est commise, en tout ou en partie, sur son territoire, et/ou b) l'auteur de l'infraction est l'un de ses ressortissants. En d'autres termes, l'article 12, paragraphe 1, point a), de la directive consacre le principe de territorialité, tandis que le point b) applique le principe de la compétence personnelle active.

L'article 13, paragraphe 1, de la directive dispose que les **outils d'enquête** utilisés aux fins des enquêtes et des poursuites concernant les infractions visées aux articles 3 à 8 devraient être efficaces, proportionnés et mis à la disposition des personnes, des unités ou des services compétents. Les informations relatives aux infractions visées aux articles 3 à 8 devraient être communiquées sans retard indu aux autorités chargées des enquêtes et des poursuites concernant ces infractions, conformément à l'article 13, paragraphe 2, de la directive.

En ce qui concerne l'échange d'informations, l'article 14 impose aux États membres de veiller à disposer de **points de contact** nationaux opérationnels, disponibles vingt-quatre heures sur vingt-quatre et sept jours sur sept, afin de pouvoir répondre dans un délai de huit heures à toute demande urgente provenant de l'étranger.

[7] Sauf indication contraire, tous les articles mentionnés sont ceux de la directive.

Par ailleurs, l'article 15, paragraphe 1, de la directive exige des États membres qu'ils mettent en place des canaux appropriés pour **signaler les infractions** visées aux articles 3 à 8 aux autorités publiques sans retard indu. Les établissements financiers sont notamment invités à signaler les soupçons de fraude aux services répressifs et aux autorités judiciaires (article 15, paragraphe 2). Le signalement est fréquemment le point de départ des enquêtes judiciaires (considérant 27).

Enfin, les articles 16 et 17 portent de la directive respectivement sur **l'aide et le soutien aux victimes** et sur la **prévention**.

1.2 Objet et méthodologie du rapport

L'article 20 de la directive prescrit aux États membres de mettre en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la directive au plus tard le 31 mai 2021 et de les communiquer à la Commission.

Le présent rapport répond à l'obligation prévue à l'article 21 de la directive, selon laquelle la Commission doit présenter au Parlement européen et au Conseil un rapport évaluant dans quelle mesure les États membres ont pris les mesures nécessaires pour se conformer à la directive. Le présent rapport, le premier présenté au titre de l'article 21, fournit un aperçu des principales mesures de transposition prises par les États membres.

La transposition par les États membres a consisté à recueillir des informations sur la législation et les mesures administratives pertinentes, à les analyser, à élaborer une nouvelle législation ou, dans la plupart des cas, à modifier des actes existants, à les adopter et enfin à en rendre compte à la Commission.

À la date limite de transposition (31 mai 2021), neuf États membres avaient notifié à la Commission l'achèvement de la transposition de la directive et lui avaient communiqué leurs mesures de transposition. En juillet 2021, la Commission a engagé des procédures d'infraction pour non-communication de mesures nationales de transposition à l'encontre des 16 autres États membres: AT, BE, BG, CY, CZ, EL, ES, HR, IT, LU, LV, MT, PL, PT, RO et SI[8]. Alors que, en date du 30 avril 2023, 15 États membres avaient notifié leurs mesures de transposition, une procédure d'infraction pour non-communication des mesures de transposition nationales est toujours en cours contre BG[9].

La description et l'analyse contenues dans la suite du présent rapport sont fondées sur les informations relatives aux mesures nationales de transposition communiquées par les États membres au plus tard le 31 janvier 2023. Les notifications reçues après cette date n'ont pas été prises en considération. Toutes les mesures notifiées faisant référence aux législations nationales ont été prises en considération, de même que les décisions de justice et, le cas échéant, la doctrine juridique communément admise. De plus, au cours de l'analyse, la Commission a directement pris contact avec les États membres lorsque cela s'est révélé

[8] Le nom des États membres mentionnés dans le présent document est abrégé comme suit: http://publications.europa.eu/code/fr/fr-5000600.htm.

[9] Pour de plus amples informations sur les décisions de la Commission relatives aux procédures d'infraction, voir: http://ec.europa.eu/atwork/applying-eu-law/infringements-proceedings/infringement_decisions/?lang_code=en.

approprié pour obtenir des informations ou des explications complémentaires. Toutes les informations collectées ont été prises en considération aux fins de l'analyse.

Au-delà des questions recensées dans le présent rapport, il se peut qu'il existe d'autres obstacles à la transposition, que d'autres dispositions n'aient pas été notifiées à la Commission ou que des évolutions législatives et non législatives futures se produisent. Le présent rapport n'empêche donc pas la Commission d'évaluer certaines dispositions de manière plus approfondie et de continuer à aider les États membres dans la transposition et la mise en œuvre de la directive.

2. Mesures de transposition

2.1 Définitions juridiques

L'article 2 de la directive établit les définitions des principaux termes employés dans la directive, à savoir: instrument de paiement autre que les espèces; dispositif, objet ou enregistrement protégé; moyens d'échange numérique; monnaie virtuelle; système d'information; données informatiques; personne morale.

De manière générale, les États membres ont transposé les définitions en s'appuyant sur des lois antérieures à la directive ou adoptées après son entrée en vigueur. Dans certains cas, en l'absence de dispositions spécifiques établissant des définitions, les infractions sont transposées dans des dispositions générales du code pénal dont la portée est plus large, par exemple les dispositions relatives au vol. Par conséquent, la non-communication d'une transposition verbatim de la définition n'indique pas nécessairement une transposition incomplète ou un défaut de conformité.

De plus, plusieurs des définitions renvoient à des définitions établies dans d'autres directives.

a) Instruments de paiement autres que les espèces

L'évaluation a révélé au moins un cas de transposition incomplète, la définition établie par la décision-cadre 2001/413/JAI du Conseil n'ayant pas été mise à jour. Par conséquent, dans ce cas, la définition fait uniquement référence aux instruments de paiement matériels et ne couvre pas les "dispositifs, objets ou enregistrements protégés [...] ou une combinaison de ces éléments", comme indiqué dans la définition de la directive.

b) Dispositif, objet ou enregistrement protégé

Plusieurs États membres n'ont pas transposé cette définition (BG, CZ, EE, ES, FI, HR, LT, NL, PL, PT, RO, SI). Il ne s'agit pas nécessairement de cas de non-respect, car, en général, le sens est évident ou peut être déduit à partir du libellé de la définition du terme "instrument de paiement autre que les espèces". Dans certains pays, le concept est expliqué dans les travaux préparatoires.

c) Moyens de paiement numériques et monnaie virtuelle

Ces deux définitions sont au cœur de la directive 2019/713, qui avait pour objectif principal de remédier au fait que la décision-cadre 2001/413/JAI ne correspondait plus aux réalités actuelles et ne tenait pas suffisamment compte des nouveaux défis et évolutions technologiques, tels que les monnaies virtuelles et les paiements mobiles, qu'il convient d'inclure pour apporter une réponse globale au phénomène et combler les lacunes involontaires apparues en matière d'incrimination.

La difficulté principale rencontrée lors de la transposition concerne la portée du terme "monnaie virtuelle", tel qu'il est défini à l'article 2, point d), de la directive. Bien que le terme "monnaie électronique" soit défini dans tous les États membres, généralement du fait de la transposition de la directive relative à la monnaie électronique[10], la définition et la portée du terme "monnaie virtuelle" ne sont pas toujours évidentes.

[10] 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).

En HU, la monnaie virtuelle est considérée comme un bien et une donnée électronique, et peut faire l'objet d'une confiscation et d'une saisie. De même, en PL, la monnaie virtuelle n'est pas définie par la loi et il existe un certain degré d'incertitude quant au fait de savoir si elle est couverte par les différentes infractions concernées par la transposition de la directive, bien que certains auteurs considèrent que la monnaie virtuelle pourrait relever des dispositions du code pénal réglementant les infractions relatives à l'information, aux supports d'information ou aux données d'information.

De nombreux États membres ont transposé ces définitions dans les règles financières plutôt que dans le droit pénal (AT, BE, BG, CY, CZ, DE, EE, EL, ES, HR, HU, LT, LU, LV, SI). Cependant, dans certains de ces cas, il est renvoyé aux dispositions pertinentes de la législation nationale qui établit les infractions. Enfin, dans trois États membres (IT, MT, RO), les deux définitions sont transposées dans le code pénal.

d) Système d'information

L'article 2, point e), définit le terme "système d'information" par référence à l'article 2, point a), de la directive 2013/40/UE. Tous les États membres ont transposé cette définition conformément à la directive.

e) Données informatiques

L'article 2, point f), définit le terme "données informatiques" par référence à l'article 2, point b), de la directive 2013/40/UE. Tous les États membres ont transposé l'article 2, point f), conformément à la directive.

f) Personne morale

Enfin, l'article 2, point g), définit le terme "personne morale". La quasi-totalité des États membres ont transposé ce terme dans leur législation, à l'exception de SE, qui ne définit pas le terme "personne morale". Le terme qui s'en rapproche le plus dans les dispositions de transposition est "entreprise". Ce terme n'est pas défini dans les textes juridiques, la doctrine ou la jurisprudence.

2.2 Infractions pénales spécifiques

a) Utilisation frauduleuse des instruments de paiement autres que les espèces

L'article 3, point a), de la directive impose aux États membres de prendre les mesures nécessaires pour ériger en infraction pénale punissable l'utilisation frauduleuse d'un instrument de paiement autre que les espèces, volé, usurpé ou obtenu par d'autres moyens illégaux, lorsqu'elle est intentionnelle.

25 États membres ont transposé l'article 3, point a), de la directive. 14 d'entre eux ont transposé la directive dans une disposition spécifique relative à l'utilisation frauduleuse des instruments de paiement autres que les espèces (AT, CY, ES, FI, HU, IT, LT, MT, NL, PT, RO, SE, SI, SK). Les autres États membres ont fait référence à des infractions plus générales, telles que la fraude et la contrefaçon reposant sur des procédés informatiques, ou la fraude liée aux moyens de paiement, sans se limiter aux instruments de paiement autres que les espèces (BE, BG, CZ, DE, EE, EL, FR, HR, LU, LV, PL, SE, SK).

La législation de HR ne fait pas référence à l'utilisation d'instruments de paiement volés ou autrement usurpés; la disposition de transposition en HU ne renvoie qu'aux instruments électroniques parmi les instruments de paiement autres que les espèces.

Conformément à l'article 3, point b), de la directive, les États membres prennent les mesures nécessaires pour ériger en infraction pénale punissable l'utilisation frauduleuse d'un instrument de paiement autre que les espèces, faux ou falsifié, lorsqu'elle est intentionnelle.

De manière générale, l'article 3, point b), a été entièrement transposé.

Pour transposer la directive, 15 États membres font référence aux dispositions nationales relatives aux instruments de paiement autres que les espèces (AT, CY, DE, EE, ES, FI, HR, HU, IT, LT, MT, NL, PT, RO, SI), tandis que, dans dix États membres, la législation nationale de transposition couvre des infractions plus générales, telles que le vol ou la fraude, ou des infractions liées à des instruments de paiement, mais pas spécifiquement des instruments de paiement autres que les espèces (BE, BG, CZ, EL, FR, LU, LV, PL, SE, SK).

b) Infractions liées à l'utilisation frauduleuse d'instruments de paiement matériels autres que les espèces

L'article 4 de la directive impose aux États membres de prendre les mesures nécessaires pour ériger en infraction pénale punissable les agissements intentionnels énumérés dans ses alinéas. Il s'agit a) du vol ou autre usurpation d'un instrument de paiement matériel autre que les espèces, b) de la contrefaçon ou de la falsification frauduleuses d'un instrument de paiement matériel autre que les espèces, c) de la possession d'un instrument de paiement matériel autre que les espèces, volé, usurpé ou obtenu par d'autres moyens illégaux ou faux ou falsifié, en vue de son utilisation frauduleuse, d) de l'obtention pour soi-même ou autrui, y compris la réception, l'appropriation, l'achat, le transfert, l'importation, l'exportation, la vente, le transport ou la diffusion, d'un instrument de paiement matériel autre que les espèces, volé, faux ou falsifié, en vue de son utilisation frauduleuse.

Bien que l'article 4 ait généralement été transposé de manière plus ou moins littérale, dans certains cas, la transposition nationale soulève des questions quant aux agissements particuliers constituant l'obtention, pour soi-même ou autrui, d'un instrument de paiement matériel autre que les espèces, volé, faux ou falsifié, en vue de son utilisation frauduleuse.

c) Infractions liées à l'utilisation frauduleuse d'instruments de paiement non matériels autres que les espèces

L'article 5 de la directive érige en infraction pénale les agissements liés à l'utilisation frauduleuse d'instruments de paiement non matériels autres que les espèces. L'analyse a révélé que la transposition de cet article n'avait pas posé de problèmes. Dans la majorité des cas, la disposition nationale s'applique aux instruments de paiement matériels et non matériels autres que les espèces. Environ la moitié des États membres ont transposé l'article 5 de la directive dans une disposition plus générale (BE, BG, DE, EE, FI, HR, FR, LV, PL, SE, SK), tandis que plus de la moitié l'ont transposé dans une disposition spécifique relative à l'utilisation frauduleuse des instruments de paiement autres que les espèces (AT, CY, CZ, EL, ES, HU, IT, LT, LU, NL, PT, RO, SI).

d) Fraude liée aux systèmes d'information

L'article 6 de la directive oblige les États membres à 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 monnaie virtuelle, causant ainsi de manière illicite à autrui une perte de propriété dans le but de procurer un gain illégal à l'auteur de l'infraction ou à un tiers, en empêchant ou en perturbant le fonctionnement d'un système informatique, sans en avoir le droit [article 6, point a)], ou en introduisant, altérant, effaçant, transmettant ou supprimant des données informatiques, sans en avoir le droit [article 6, point b)]. Tous les États membres ont transposé l'article 6.

e) Outils utilisés pour commettre les infractions

L'article 7 de la directive exige que les États membres prennent les mesures nécessaires pour ériger en infraction pénale punissable la production, l'obtention pour soi-même ou pour autrui, ou la mise à disposition d'un dispositif ou d'un instrument, de données informatiques ou d'autres moyens principalement conçus ou spécifiquement adaptés pour commettre l'une des infractions visées à l'article 4, points a) et b), à l'article 5, points a) et b), ou à l'article 6, au moins lorsqu'elles sont commises dans l'intention que ces moyens soient utilisés.

La grande majorité des États membres ont transposé l'article 7 de la directive (AT, CY, CZ, DE, EE, ES, FI, FR, HR, IT, LT, LV, NL, RO, SE, SI, SK).

Six pays ont transposé l'article 7 de la directive dans des dispositions qui renvoient à des dispositions plus générales, relatives à des infractions générales comme le vol ou concernant des instruments financiers et des moyens de paiement (BG, FI, FR, LV, SE, SK). 17 pays l'ont transposé dans une disposition spécifique relative aux outils utilisés pour commettre les différentes infractions visées par la directive en lien avec des instruments de paiement matériels et non matériels autres que les espèces (AT, CY, CZ, DE, EE, EL, ES, HR, HU, IT, LT, LU, MT, NL, PL, RO, SI).

Cinq États membres ont rencontré des difficultés pour transposer cet article (BE, BG, HU, PL, PT).

2.3 Règles générales relatives aux infractions concernées

a) Instigation, complicité et tentative

Conformément à l'article 8, paragraphe 1, de la directive, les États membres doivent veiller à ériger en infraction pénale punissable l'instigation d'une infraction visée aux articles 3 à 7 ou le fait de s'en rendre complice.

Tous les États membres ont transposé cette disposition. La grande majorité des États membres ont transposé la directive dans un article préexistant sur l'instigation et la complicité en général (AT, BE, BG, CZ, DE, EE, EL, ES, FI, FR, HR, HU, IT, LT, LU, LV, NL, PL, PT, RO, SE, SI, SK). Cependant, deux États membres ont décidé d'adopter une nouvelle disposition, qui s'applique uniquement dans le cadre des infractions visées par la directive (CY, MT).

La première phrase de l'article 8, paragraphe 2, de la directive impose aux États membres de veiller à ériger en infraction pénale punissable une tentative de commettre une infraction visée à l'article 3, à l'article 4, point a), b) ou d), à l'article 5, point a) ou b), ou à l'article 6. Tous les États membres ont transposé cette disposition dans son entièreté, à l'exception de BE, LU et SI.

Là encore, la majorité des États membres ont transposé la directive dans une disposition préexistante relative à la tentative en général (AT, BG, CZ, EE, EL, ES, FR, HR, HU, IT, LT, LV, NL, PL, PT, SE, SK). Les autres États membres ont intégré cette disposition à une mesure de transposition spéciale (CY, DE, FI, MT, RO).

Les États membres doivent également veiller à ériger en infraction pénale punissable au moins la tentative d'obtention frauduleuse d'un instrument de paiement non matériel autre que les espèces obtenu par des moyens illégaux, falsifié ou faux, pour soi-même ou autrui [article 5, point d), et article 8, paragraphe 2, deuxième phrase].

Il est ressorti de l'évaluation que, dans deux États membres (HR, SI), l'incrimination de la tentative peut faire l'objet de restrictions non prévues par la directive.

Tous les autres États membres ont transposé les dispositions pertinentes de la directive, dans un article sur la tentative en général (AT, BE, BG, CZ, IT, EE, EL, ES, FR, HU, LT, LU, LV, NL, PL, PT, SE, SK) ou dans une mesure de transposition spéciale (CY, DE, FI, MT, RO).

b) Sanctions

L'article 9 dispose que les infractions visées aux articles 3 à 8 sont passibles de sanctions pénales effectives, proportionnées et dissuasives et précise la peine d'emprisonnement maximale pour chaque infraction.

Bien que la plupart des États membres aient transposé l'article 9 de la directive, l'évaluation a mis en lumière des problèmes éventuels en rapport avec le champ d'application de la définition pour l'article 9, paragraphe 2 (HR) et l'article 9, paragraphe 6 (BE, CZ, HR, HU).

Il est difficile de comparer les sanctions prévues par les États membres pour les différentes infractions, car ces dernières relèvent à la fois de dispositions générales et spécifiques. Lorsqu'ils ont transposé la directive dans des dispositions relatives à des infractions générales, les États membres se sont appuyés sur plusieurs dispositions nationales pour ériger en infraction pénale l'un des agissements interdits par la directive. Il s'ensuit que plusieurs peines maximales sont applicables à cette infraction spécifique et que la sanction maximale réelle dépendra de chaque cas concret, de l'approche adoptée par les juridictions et des règles nationales relatives au cumul des sanctions. Par exemple, en PL, la règle veut qu'un agissement ne puisse constituer qu'une seule infraction. Même si un agissement présente des caractéristiques propres à deux ou plusieurs dispositions du code pénal, la juridiction ne doit retenir qu'une seule infraction. Au contraire, en BG, lorsque la section spéciale du code pénal prévoit d'imposer plusieurs sanctions pour un certain type d'infraction, la juridiction doit déterminer la mesure de chaque sanction afin que leur somme corresponde aux objectifs généraux de la sanction.

En outre, les dispositions peuvent prévoir des circonstances aggravantes susceptibles de donner lieu au relèvement du plafond et à l'alourdissement des peines. La sanction maximale dépend donc de la manière dont l'infraction est commise. Par exemple, en HR, la disposition générale relative au détournement prévoit une peine d'emprisonnement maximale de cinq ans. Cependant, si l'auteur de l'infraction a recours à la force, l'infraction est passible d'une peine maximale de 10 ans, et si elle entraîne un gain matériel important, l'auteur de l'infraction encourt une peine d'emprisonnement de 12 ans. En DE, la falsification d'instruments de paiement matériels autres que les espèces est passible d'une peine d'emprisonnement maximale de cinq ans. Toutefois, si l'auteur de l'infraction a agi à des fins commerciales, il est passible d'une peine maximale de 10 ans.

L'évaluation a également révélé que, dans la plupart des cas, les peines maximales prévues par la législation nationale sont plus sévères que celles établies par la directive. Les différences peuvent être importantes: la contrefaçon est passible d'une peine d'emprisonnement pouvant aller jusqu'à 15 ans en BG et au LU et jusqu'à 25 ans en PL. Seuls deux États membres (AT, MT) prévoient les mêmes (ou quasiment les mêmes) peines maximales que la directive.

c) Responsabilité des personnes morales

L'évaluation a montré que 16 États membres avaient transposé l'article 10 de la directive dans une disposition générale préexistante de leur code pénal (AT, CZ, BE, BG, DE, EE, ES, FR, HR, HU, LU, LV, NL, PT, RO, SE), tandis que neuf États membres l'ont transposé dans une loi spécifique relative à la responsabilité des personnes morales dans le cadre de la directive (CY, EL, FI, IT, LT, MT, PL, SI, SK).

d) Sanctions à l'encontre des personnes morales

L'article 11 de la directive impose aux États membres de prévoir également pour les personnes morales des sanctions effectives, proportionnées et dissuasives sous la forme d'amendes pénales ou non pénales. Tous les États membres ont prévu de telles sanctions.

L'article 11 donne aux États membres la possibilité de prévoir diverses sanctions spécifiques à l'encontre des personnes morales, telles que l'exclusion du bénéfice d'un avantage public ou une mesure judiciaire de dissolution. Six États membres n'ont pas du tout eu recours à l'option visée à l'article 11 de la directive (AT, BG, EE, FI, NL, SE). Les 19 autres pays ont transposé l'article 11 en tout ou en partie (BE, CY, CZ, DE, EL, ES, FR, HR, HU, IT, LT, LU, LV, MT, PL, PT, RO, SI, SK).

e) Compétence

Cet article, qui oblige les États membres à établir leur compétence à l'égard des infractions commises sur leur territoire ou par un de leurs ressortissants, est transposé dans les dispositions générales du code pénal national ou du code de procédure pénale national dans tous les États membres. Par conséquent, le principe de territorialité et le principe de la compétence personnelle active sont d'application générale et ne sont pas spécifiques aux infractions relevant de la directive. De plus, l'article 12 a également été transposé par CY dans sa législation nationale sur la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces et par PT dans sa loi relative à la cybercriminalité.

Tous les États membres ont transposé l'article 12, paragraphe 1, points a) et b).

L'article 12, paragraphe 3, permet aux États membres d'établir leur compétence à l'égard d'une infraction visée aux articles 3 à 8 de la directive qui a été commise en dehors de leur territoire lorsque, entre autres, a) l'infraction est commise par une personne résidant habituellement sur leur territoire, b) l'infraction a été commise pour le compte d'une personne morale établie sur leur territoire, ou c) l'infraction a été commise à l'encontre de l'un de leurs ressortissants ou d'une personne résidant habituellement sur leur territoire. Quatorze États membres (BE, CY, CZ, DE, EL, ES, FI, HR, LT, LV, MT, NL, SE, SK) ont fait usage de la faculté prévue à l'article 12, paragraphe 3, point a), 12 États membres (BE, CY, CZ, EL, FI, LV, MT, NL, PL, PT, SI, SK) ont transposé l'article 12, paragraphe 3, point b), et 16 États membres (AT, BG, CY, CZ, DE, EE, EL, FI, FR, HR, HU, LV, MT, RO, SE, SI) ont étendu leur compétence conformément à l'article 12, paragraphe 3, point c). En ce qui concerne le point c), BG, DE, EE, HU, RO et SI ont établi leur compétence à l'égard d'une infraction commise en dehors de leur territoire lorsque l'infraction est commise (uniquement) à l'encontre de l'un de leurs ressortissants (ignorant ainsi les personnes résidant habituellement sur leur territoire). AT prévoit que les infractions commises à l'étranger font l'objet de poursuites par le système de justice pénale autrichien si l'auteur de l'infraction et la victime sont autrichiens. CY, CZ, EL, FI, LV et MT ont fait usage des trois facultés prévues à l'article 12, paragraphe 3.

2.4 Questions opérationnelles

a) Efficacité des enquêtes et de la coopération

Dans tous les États membres, les outils d'enquête destinés à mener les enquêtes et à exercer les poursuites en ce qui concerne les infractions visées aux articles 3 à 8 ne sont pas explicitement mentionnés dans la législation transposant la directive, mais plutôt dans une législation plus générale, telle que les codes de procédure pénale. Généralement, la possibilité d'utiliser un outil d'enquête dans un cas déterminé est liée à la sanction prévue pour l'infraction en question; par conséquent, comme indiqué dans la disposition de la directive, les outils d'enquête qui sont utilisés dans les affaires de lutte contre la criminalité organisée ou d'autres formes graves de criminalité seront également mis à disposition pour mener des enquêtes et exercer des poursuites en ce qui concerne les infractions définies dans la directive. Le caractère exceptionnel de certains outils d'enquête et la nécessité de la proportionnalité avec l'infraction sont généralement précisés dans les dispositions juridiques pertinentes et/ou dans la Constitution.

Les informations relatives aux infractions visées aux articles 3 à 8 devraient être communiquées sans retard indu aux autorités chargées des enquêtes et des poursuites concernant ces infractions, conformément à l'article 13, paragraphe 2, de la directive. En d'autres termes, les services répressifs et les autres autorités compétentes devraient avoir accès, en temps utile, aux informations pertinentes pour mener les enquêtes et exercer les poursuites en ce qui concerne les infractions visées dans la directive (considérant 22). Le code de procédure pénale prévoit souvent divers systèmes de signalement pour que les infractions pénales (au sens des articles 3 à 8 de la directive) puissent être signalées efficacement et rapidement. Ces systèmes de signalement incluent: une obligation de signalement incombant aux entités et autorités publiques, un système de dénonciation des infractions, une procédure de plainte, l'obligation pour les prestataires de services de paiement de signaler les incidents graves ayant trait à l'exploitation ou à la sécurité, et le droit pour les particuliers de signaler des incidents. Par ailleurs, des législations plus spécifiques peuvent garantir que les signalements d'incidents ayant trait à la sécurité (notamment, signalements d'actes criminels graves, tels que l'obtention non autorisée, la falsification et l'altération d'un moyen de paiement) sont communiqués aux autorités compétentes aussi rapidement que possible. AT, CZ, LT, FI, MT et PT ont indiqué s'être dotés de ce type de législation.

La condition selon laquelle "les autorités compétentes reçoivent lesdites informations sans retard indu" n'est généralement pas transposée de façon explicite.

b) Échange d'informations

L'échange d'informations entre les services répressifs nationaux dans le cadre des enquêtes et des poursuites menées à l'égard des infractions, y compris des infractions visées aux articles 3 à 8 de la directive, peut être facilité grâce aux points de contact opérationnels (considérant 26). Conformément à l'article 14, paragraphe 1, première phrase, de la directive, les États membres doivent établir effectivement ces points de contact, qui doivent être disponibles vingt-quatre heures sur vingt-quatre, sept jours sur sept. La deuxième phrase impose aux États membres de mettre des procédures en place pour traiter rapidement les demandes urgentes d'assistance et pour qu'il y soit répondu dans un délai de huit heures, en indiquant au moins si la demande sera satisfaite et la forme d'une telle réponse ainsi que le délai estimé dans lequel elle sera envoyée.

Les États membres suivants ont décidé de recourir à un point de contact opérationnel existant aux fins décrites dans la directive: AT, BE, CY, EE, EL, ES, FR, HU, IT, LT, LV, NL, PL, PT, SE.

Le tableau nº 1 fournit un aperçu des points de contact existants. Aucun point de contact n'a été recensé dans les pays suivants: BG, CZ, LU, SI, HR.

Tableau nº 1 Points de contact opérationnels

ÉM	Point de contact	ÉM	Point de contact
AT	Office fédéral de la police criminelle	**EE**	Ministère de la justice
BE	Direction de l'information policière opérationnelle	**FI**	Bureau national du renseignement
BG	s.o.	**FR**	Division des relations internationales de la direction centrale de la police judiciaire
CY	Police chypriote	**HR**	s.o.
CZ	s.o.	**HU**	Centre international de coopération pénale (NEBEK)
DE	16 bureaux fédérés de la police criminelle et 1 bureau fédéral de la police criminelle – points de contact centraux de lutte contre la	**MT**	Police maltaise

	cybercriminalité		
EL	Police grecque (division de la coopération policière internationale)	**ES**	Cellule de coordination d'urgence
IT	Département des opérations internationales du service de la coopération policière internationale	**NL**	Centre national d'assistance juridique internationale (LIRC)
LT	2e division du conseil de gestion des forces de la direction de la police relevant du ministère de l'intérieur de la République de Lituanie et du comité des relations internationales du bureau lituanien de la police judiciaire	**PL**	Direction générale de la police
LV	Police nationale	**PT**	Police judiciaire
RO	Section des enquêtes judiciaires et des poursuites du bureau du procureur général	**SE**	Autorité policière
SI	s.o.	**SK**	Bureau de la police judiciaire du présidium des forces de police de la République slovaque

L'article 14, paragraphe 1, deuxième phrase, de la directive a été mis en œuvre en pratique dans quelques États membres. Aucune information relative aux procédures à appliquer aux demandes urgentes n'a pu être trouvée en BE, BG, CZ, LV, RO, FR, HR, LU, NL, PL, SE, SK.

c) Signalement des infractions

Les États membres sont également obligés de mettre à disposition des canaux de communication appropriés. Les canaux utilisés pour signaler les soupçons de fraude ou, plus généralement, les infractions pénales potentielles, peuvent être prévus par des actes législatifs. Souvent, les États membres ont érigé en obligation le signalement des infractions pour certaines catégories de personnes (physiques et morales) (dans le droit fil de l'article 15, paragraphe 2), tandis que les victimes et autres "observateurs" ont la possibilité (mais pas l'obligation) d'effectuer un signalement. Ces dispositions juridiques sont généralement complétées par une mise en œuvre concrète.

Dans tous les États membres, des signalements écrits ou oraux peuvent être effectués auprès de la police ou du pouvoir judiciaire. Par ailleurs, certains États membres ont prévu des canaux de communication supplémentaires:

Le droit fédéral de AT prévoit plusieurs systèmes de signalement permettant de signaler efficacement et rapidement les infractions pénales au sens des articles 3 à 8 de la directive: 1) obligation de signalement incombant aux entités et autorités publiques, 2) système de dénonciation du bureau du procureur général en charge des affaires économiques et de la lutte contre la corruption, 3) système de dénonciation de l'autorité des marchés financiers, et 4) obligation pour les prestataires de services de paiement de signaler les incidents graves ayant trait à l'exploitation ou à la sécurité. Un bureau de signalement des actes de cybercriminalité a été mis en place par le bureau fédéral de la police judiciaire. De plus, le ministère fédéral de l'intérieur coopère avec la chambre économique fédérale. En conséquence, plusieurs campagnes et envois de messages sont organisés pour encourager et inciter le public à signaler des violations pertinentes du droit.

En BE, le ministère de l'économie gère un point de contact unique pour les victimes de fraude, d'arnaque, de tromperie et d'escroquerie. Par ailleurs, un canal de dénonciation a été juridiquement constitué et mis à disposition par l'autorité des services et marchés financiers pour toutes les plaintes liées à des produits et services de crédit ou d'investissement.

À CY, la police chypriote, ainsi que la Banque centrale de Chypre et l'autorité nationale chargée de la sécurité des réseaux et des systèmes d'information, sont officiellement désignés, par une mesure législative, comme les autorités nationales compétentes chargées de la mise en place des canaux appropriés de signalement et de communication.

Le droit pénal de CZ oblige les autorités publiques à signaler des infractions.

En DE, les entités concernées sont tenues de signaler les transactions suspectes sans délai indu. En outre, des mesures non législatives ont été adoptées au niveau fédéral, telles que la création d'un partenariat public-privé institutionnalisé aux fins de la détection et de la prévention des infractions visées aux articles 3 à 8 de la directive ainsi que des enquêtes et des poursuites en la matière, et d'une plateforme pour l'échange d'informations.

En EL, outre les canaux de communication généraux, le gouvernement grec a mis en place un service public en ligne qui permet aux citoyens de porter plainte directement en cas d'infractions pénales commises en ligne. En outre, les établissements de crédit et autres prestataires de services de paiement sont tenus de signaler immédiatement tout cas de fraude à la Banque de Grèce (qui est habilitée à traiter ce type de plaintes).

En ES, outre les canaux généraux de signalement des infractions, la Banque d'Espagne met à disposition un canal de communication en collaboration avec l'Institut national de cybersécurité.

La législation italienne garantit la rapidité de la communication des informations relatives à une infraction au procureur général par la police judiciaire, que cette dernière ait obtenu l'information de sa propre initiative ou que le signalement fasse suite à une plainte ou à une procédure civile. L'échange d'informations est également encouragé par l'intermédiaire des plateformes numériques.

LT dispose de plusieurs canaux de communication pour signaler les infractions visées aux articles 3 à 8 de la directive: page web (portail électronique de la police), numéro général d'appel d'urgence (112), en personne, courrier électronique, message SMS, application mobile de la police et autres moyens automatisés. Les prestataires de services de paiement, les établissements financiers et les autres entités concernées, la Banque de Lituanie et le service d'enquête sur la criminalité financière sont tenus de communiquer aux services répressifs compétents tout soupçon raisonnable d'infraction pénale et/ou d'autres agissements délictueux.

Au LU, un site web qui explique comment signaler les fraudes est disponible. La commission de surveillance du secteur financier a élaboré des lignes directrices pour détecter les fraudes financières mais elle exige aussi de tous les établissements qui relèvent de son contrôle qu'ils lui signalent dès que possible tout cas de fraude et tout incident dû à des attaques informatiques extérieures.

En RO, les fonctionnaires, les personnes qui occupent des postes de direction au sein des autorités publiques, les personnes qui fournissent des services d'intérêt public et les personnes qui travaillent au sein d'organes de contrôle et de supervision ont l'obligation de signaler les infractions.

En SI, toutes les autorités nationales et organisations dépositaires de l'autorité publique sont tenues de signaler les infractions.

En FR, la plateforme "Perceval", établie par un acte juridique, permet aux victimes de signaler les fraudes à la carte bancaire ainsi que les actes de contrefaçon. Une plateforme semblable permet de signaler les actes de cybercriminalité. Par ailleurs, des sanctions s'appliquent à toute personne (physique ou morale) qui n'empêche pas, par son action immédiate, la commission d'une infraction, ce qui entraîne une obligation générale de signalement.

En HU, seuls les membres de l'autorité, les fonctionnaires publics et les organismes professionnels légaux sont tenus de signaler les infractions pénales. Sur son site web, la Banque nationale hongroise encourage, sous la forme d'un avis, les établissements financiers à signaler les soupçons de fraude.

À MT, le point de contact national encourage, en particulier, les établissements financiers à signaler les soupçons de fraude et de contrefaçon des moyens de paiement autres que les espèces.

Au PT, outre le canal de communication juridiquement constitué, il existe un système de signalement de la cybercriminalité qui permet, "en un seul clic", de suivre un lien qui ouvre instantanément un courrier électronique destiné aux autorités compétentes.

En SE, certains types d'infraction, tels que la fraude à la carte de crédit, peuvent être signalés grâce au service électronique de l'autorité policière. Par ailleurs, les acteurs du système bancaire et financier sont tenus de signaler à l'autorité policière les activités suspectes liées à des cas potentiels de blanchiment d'argent ou de financement du terrorisme, ou les biens provenant par d'autres voies d'une activité criminelle. De plus, le système bancaire et financier et le Centre national de lutte contre la fraude de l'autorité policière maintiennent un dialogue constant.

En SK, des dispositions juridiques établissent l'obligation (et les procédures) pour les autorités publiques et les autres personnes morales de signaler les infractions pénales aux services répressifs dans les plus brefs délais. Certaines entités, et notamment les banques, sont également tenues de signaler le blanchiment d'argent.

Par ailleurs, des mesures non législatives mettant en œuvre l'article 15 de la directive ont été adoptées par NL et PL. Les lignes téléphoniques et le site web de la police néerlandaise constituent un canal approprié pour signaler aux autorités les cas de fraude qui concernent des moyens de paiement autres que les espèces. En outre, le gouvernement néerlandais s'est engagé à encourager les établissements financiers et les autres personnes morales à signaler tout soupçon de fraude. En témoigne, par exemple, la présence d'un guichet chargé de la fraude financière dans toutes les unités de police aux Pays-Bas. De plus, quatre grandes banques et la société ICS ont signé une convention avec la police en vue de lutter conjointement contre la fraude (bancaire) et le hameçonnage. En PL, les infractions peuvent être signalées vingt-quatre heures sur vingt-quatre, sept jours sur sept, à toutes les unités de police. En outre, compte tenu de la nature des infractions commises au moyen de technologies informatiques, il est possible d'entrer directement en contact avec une unité organisationnelle spécialisée de la direction générale de la police. Par ailleurs, afin de garantir la coopération la plus rapide possible avec le secteur bancaire, un canal de coopération a été mis sur pied entre le bureau de lutte contre la cybercriminalité de la direction générale de la police et le centre de sécurité bancaire de l'Association bancaire polonaise.

L'article 15, paragraphe 2, de la directive n'a pas été transposé en BG, EE, HR.

2.5 Soutien aux victimes et prévention

a) Aide et soutien aux victimes

L'aide et le soutien aux personnes physiques et morales dont les données à caractère personnel ont fait l'objet d'une utilisation abusive sont garantis par l'article 16, paragraphe 1, de la directive. Les mesures devraient comprendre: a) la mise à disposition d'informations et de conseils sur la protection contre les conséquences négatives de ces infractions, et b) la mise à disposition d'une liste d'établissements s'occupant spécifiquement des divers aspects des infractions relatives à l'usurpation d'identité et du soutien aux victimes.

Dans le même ordre d'idées, les personnes morales qui sont victimes des infractions visées aux articles 3 à 8 de la directive devraient avoir accès aux informations concernant a) les procédures de dépôt de plainte, b) le droit de recevoir des informations sur leur dossier, c) les procédures disponibles pour introduire une réclamation si l'autorité compétente ne respecte pas les droits de la victime au cours de la procédure pénale, et d) les coordonnées utiles pour l'envoi de communications relatives à leur dossier (article 16, paragraphe 3, de la directive).

Dans la plupart des États membres, le code de procédure pénale contient des dispositions relatives aux victimes et à leurs droits, notamment certaines dispositions spécifiques concernant les droits des victimes à l'information et à une assistance au cours de la procédure, le droit de se faire assister d'un conseil et le droit de déposer plainte. Une loi spécifique transposant la directive complète souvent ce qui figure déjà dans le code de procédure pénale. Les personnes morales font généralement l'objet de dispositions juridiques distinctes, dans le code de procédure pénale ou autre. En outre, pour soutenir et aider les victimes des infractions visées aux articles 3 à 8 de la directive, il existe plusieurs campagnes d'information, brochures, sites web spécifiques, prospectus, etc. Tel est le cas pour AT, BE (en ce qui concerne l'article 16, paragraphe 1), CY, CZ, DE, IT, LT, LU (en ce qui concerne l'article 16, paragraphe 1), LV (en ce qui concerne l'article 16, paragraphe 3), RO, SI (en ce qui concerne l'article 16, paragraphe 3), EE, FI (en ce qui concerne l'article 16, paragraphe 1), FR (en ce qui concerne l'article 16, paragraphe 1), HR, HU, NL, PL (en ce qui concerne l'article 16, paragraphe 3), PT, SE et SK. L'article 16, paragraphe 1, et/ou l'article 16, paragraphe 3, de la directive n'ont été transposés littéralement ou presque dans aucun État membre, à l'exception de MT.

La liste des établissements de conseil accrédités qui fournissent une aide aux victimes, tels que visés à l'article 16, paragraphe 1, point b), de la directive, est normalement disponible en ligne et, partant, mise en œuvre dans la pratique.

b) Prévention

L'article 17 relatif à la prévention impose aux États membres de prendre des mesures appropriées, telles que des campagnes d'information et de sensibilisation et des programmes de recherche et d'éducation. La présente section s'appuie sur une évaluation des informations qui ont été communiquées par les États membres à la Commission ainsi que sur une recherche en ligne effectuée dans la documentation librement disponible pour déterminer l'existence de mesures de prévention. Comme indiqué dans le tableau nº 2 ci-dessous, les mesures de prévention qui ont été recensées ont principalement trait à la cybercriminalité et à la fraude en ligne. Cependant, dans certains pays, des informations relatives à la prévention des fraudes sont également fournies, généralement par la police.

Tableau nº 2 Mesures de prévention

ÉM	Mesures
AT	Sur son site web et les réseaux sociaux, la police fédérale donne régulièrement des informations sur la manière de se protéger contre la fraude. La coopération avec d'autres parties prenantes telles que la Chambre de commerce est renforcée et mise en œuvre dans le cadre de projets de commerce électronique.
BE	Existence de plusieurs sites web fournissant des conseils et proposant du matériel de sensibilisation, tels que ceux gérés par le Centre pour la cybersécurité Belgique (CCB). Une recherche en ligne a permis de mettre au jour une coopération avec des parties prenantes, par exemple l'organisation représentant le secteur financier a coopéré avec le parquet de Bruxelles pour concevoir du matériel de sensibilisation.
BG	Une campagne visant à lutter contre les "mules financières" en Bulgarie a été lancée en 2021 par l'Association des banques et menée conjointement avec la direction générale "Lutte contre la criminalité organisée" et le ministère public. La direction générale a, par ailleurs, lancé une

	campagne sur le hameçonnage.
CY	Le service "Cybercriminalité" de la police fournit sur son site web des informations et des conseils concernant des questions telles que la fraude numérique, mais aussi des renseignements sur les événements à venir, notamment les campagnes de sensibilisation. Exemple: la campagne d'information sur la sécurité de l'information menée par la police, les banques centrales, l'Association bancaire et l'Autorité de la sécurité numérique.
DE	La police fédérale (BKA) met à disposition sur son site web un aperçu des mesures visant à nouer des partenariats public-privé institutionnalisés aux fins de la détection et de la prévention des infractions visées par la directive ainsi que des enquêtes et des poursuites en la matière. Exemple: le partenariat entre l'Office fédéral de la police judiciaire (BKA), l'Office fédéral de la sécurité de l'information (BSI) et le Centre allemand de compétences contre la cybercriminalité e.V. (G4C), une association d'établissements financiers et d'entreprises du secteur de la sécurité informatique. Le BKA a également organisé la conférence C³ sur la cybercriminalité, une plateforme d'échange entre les autorités, les entreprises, le monde scientifique et les responsables politiques. Par ailleurs, le G4C conçoit des brochures d'information et des formations. Enfin, le BKA participe à l'élaboration de mesures de prévention en matière de cybercriminalité au niveau des Länder. Au niveau national, le BKA est également en relation avec d'autres autorités et organisations policières et non policières (parties prenantes) et œuvre au renforcement de la coopération, notamment en ce qui concerne les sujets d'actualité.
FR	Le ministère de l'intérieur publie des informations sur la prévention en matière de cybercriminalité. Des plateformes permettent de signaler les actes de cybercriminalité. Elles diffusent aussi des messages de prévention, tout comme le service d'information et de communication de la police nationale (SICoP). Citons également les lignes directrices élaborées par la Banque de France ou le guide de prévention contre les arnaques, publié par la task-force nationale de lutte contre les arnaques, qui regroupe différentes autorités administratives et répressives.
EL	À l'aide de campagnes télévisées, de discours pédagogiques et d'informations en ligne, le service "Cybercriminalité" et la direction générale de la police s'emploient à informer très activement les citoyens, à les sensibiliser et à réduire le risque d'être victime de fraude.
ES	L'Institut national espagnol de cybersécurité et l'administration fiscale mettent à disposition sur leur site web des informations pertinentes visant à éviter le hameçonnage, les logiciels rançonneurs, etc. dans les environnements professionnels.
HR	Le ministère de l'intérieur fournit des informations en ligne concernant les fraudes sur l'internet et gère une chaîne Youtube consacrée à la fraude et à la sécurité informatique, qui propose des vidéos sur les arnaques en ligne.
IT	Le ministère des finances, qui a pour mission d'éviter la fraude aux moyens de paiement, promeut déjà une série d'initiatives au niveau local, en collaboration avec les administrations locales et le monde universitaire, en organisant des séminaires et des ateliers destinés aux catégories concernées par le faux monnayage, notamment les citoyens.
LT	Des informations sur la prévention des fraudes en ligne sont disponibles sur le site web de l'Autorité de régulation des communications, tandis que le site web de la police contient des informations relatives aux types les plus courants d'escroqueries en ligne. Par ailleurs, la stratégie nationale en matière de cybercriminalité a notamment pour objectif de renforcer la prévention et le contrôle de la cybercriminalité, en particulier en renforçant la coopération entre les services répressifs et les autres parties prenantes.
LV	La commission "Marchés financiers et des capitaux" a élaboré plusieurs outils en ligne pour fournir des informations et des orientations concernant la fraude et la sécurité financière. Par ailleurs, plusieurs campagnes ont été organisées en coopération avec la police nationale et le centre de protection des droits des consommateurs.
NL	Des mesures sont en place, telles que le "Fraudehelpdesk" (permanence téléphonique en cas de fraude), un organisme subventionné par le gouvernement néerlandais auprès duquel les agissements frauduleux peuvent être signalés. Le Fraudehelpdesk fait partie de la Fondation SAFECIN (fondation de lutte contre la criminalité économique et financière aux Pays-Bas), qui bénéficie de la participation du gouvernement.
SE	Le système bancaire et financier et le Centre national de lutte contre la fraude (NBC) de l'autorité policière maintiennent un dialogue constant. Par ailleurs, le NBC collabore par exemple avec des acteurs du commerce électronique, notamment à des fins de prévention des infractions. Ces contacts soulignent l'importance de signaler les fraudes à la police.

Dans dix États membres (CZ, EE, FI, HU, MT, PL, PT, RO, SI, SK), aucune information concernant des mesures de prévention appropriées et leur mise en œuvre concrète n'a été recueillie, bien qu'à MT et en RO, la législation reflète cette obligation, avec une formulation proche de celle de la directive.

3. Conclusion et prochaines étapes

La directive a permis d'accomplir des progrès substantiels en matière d'incrimination de la fraude et de la contrefaçon des moyens de paiement autres que les espèces à un niveau comparable dans tous les États membres, ce qui facilite la coopération transfrontière entre les autorités répressives qui enquêtent sur ce type d'infractions. Les États membres ont modifié leurs codes pénaux et leur législation applicable, ils ont rationalisé leurs procédures et ils ont mis en place ou amélioré leurs programmes de coopération. La Commission reconnaît les efforts considérables déployés par les États membres pour transposer la directive.

Toutefois, il reste encore beaucoup à faire pour que la directive atteigne son plein potentiel et que les États membres en appliquent pleinement toutes les dispositions. Il ressort pour le moment de l'analyse que les principaux progrès à accomplir par les États membres concernent notamment l'article 2, point d), qui définit le terme "monnaie virtuelle", l'article 7, relatif aux outils utilisés pour commettre les infractions, et l'article 8, paragraphe 2, relatif à la tentative, l'article 9, paragraphe 6, relatif aux sanctions à l'encontre des personnes physiques dans le cas où l'infraction est commise dans le cadre d'une organisation criminelle, l'article 14, relatif à l'échange d'informations, et l'article 16, relatif à l'aide et au soutien aux victimes.

La Commission continuera de soutenir les États membres dans leur mise en œuvre de la directive. Un appel à propositions spécifique sera notamment publié en 2023.

La Commission est résolue à faire en sorte que la transposition soit parachevée dans l'ensemble de l'Union et que les dispositions soient correctement appliquées. Cela implique notamment de contrôler que les mesures nationales sont conformes aux dispositions correspondantes de la directive. Si nécessaire, la Commission exercera les pouvoirs d'exécution que lui confèrent les traités, au moyen de procédures d'infraction.