COMMISSION
EUROPÉENNE

Bruxelles, le 13.9.2017
COM(2017) 474 final

RAPPORT DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

évaluant dans quelle mesure les États membres ont pris les dispositions nécessaires pour se conformer à la directive 2013/40/UE relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil

Table des matières

1. Introduction 3
1.1. Objectifs et portée de la directive 3
1.2 Objet et méthodologie du rapport 5
2. Mesures de transposition 6
2.1 Définitions juridiques (article 2 de la directive) 6
a) Système d'information 6
b) Données informatiques 7
c) Personne morale 7
d) Sans droit 7
2.2 Infractions pénales spécifiques (articles 3 à 7 de la directive) 7
a) Accès illégal à des systèmes d'information 7
b) Atteinte illégale à l'intégrité d'un système 7
c) Atteinte illégale à l'intégrité des données 8
d) Interception illégale 8
e) Outils utilisés pour commettre les infractions 8
2.3 Règles générales relatives aux infractions concernées (articles 8 à 12 de la directive) ... 9
a) Incitation, participation et complicité 9
b) Tentative 9
c) Sanctions 9
d) Responsabilité des personnes morales 11
e) Sanctions à l'encontre des personnes morales 11
f) Compétence 12
2.4 Questions d'ordre opérationnel (articles 13 et 14 de la directive) 12
a) Disposition relative aux points de contact nationaux opérationnels 12
b) Informations relatives aux points de contact nationaux opérationnels établis 13
c) Canaux de communication 13
d) Collecte de données statistiques 13
e) Transmission des statistiques à la Commission 13
3. Conclusions et étapes suivantes 13

1. Introduction

D'après l'évaluation de la menace que représente la criminalité organisée sur l'internet (iOCTA) réalisée par Europol en 2016, la cybercriminalité devient de plus en plus agressive et conflictuelle. Cette tendance se retrouve dans différentes formes de cybercriminalité, notamment les attaques contre les systèmes d'information[1]. Europol mentionne certaines formes graves d'attaques, comme le recours à des logiciels malveillants ou à l'ingénierie sociale pour infiltrer un système d'information puis en prendre le contrôle ou pour intercepter des communications, ou le lancement d'attaques à grande échelle contre des réseaux, visant notamment les infrastructures critiques. Ces attaques constituent des menaces majeures pour notre société.

Dès lors que de plus en plus d'informations sont stockées en nuage et que les informations et les auteurs d'infractions sont extrêmement mobiles, la coopération transfrontière entre les autorités répressives est désormais cruciale pour la plupart des enquêtes en matière de cybercriminalité.

Afin de lutter de manière efficace contre ces infractions, les États membres doivent parvenir à une définition commune de ce qu'est une attaque contre les systèmes d'information. 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 12 août 2013, le Parlement européen et le Conseil ont adopté la directive 2013/40/UE relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil (ci-après la «directive»)[2].

1.1. Objectifs et portée de la directive

La directive a pour objectif de rapprocher le droit pénal des États membres[3] en matière d'attaques contre les systèmes d'information et d'améliorer la coopération entre les autorités compétentes. À cette fin, la directive fixe des règles minimales concernant la définition des infractions pénales et les sanctions en matière d'attaques contre les systèmes d'information et impose l'existence de points de contact opérationnels vingt-quatre heures sur vingt-quatre et sept jours sur sept.

En ce qui concerne la **définition** des termes pertinents, la directive mentionne:

- un «système d'information» à l'article 2, point a)[4]. La définition est proche de la définition d'un système informatique donnée à l'article 1, point a, de la convention sur la cybercriminalité du Conseil de l'Europe du 23 novembre 2001 (ci-après la

[1] Europol, 2016, Évaluation de la menace que représente la criminalité organisée sur l'internet (iOCTA), disponible à l'adresse suivante: https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2016.pdf

[2] http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32013L0040&from=FR

[3] Dans ce qui suit, sauf mention contraire explicite, les termes «États membres» ou «tous les États membres» désignent les États membres liés par la directive, à savoir tous les États membres de l'Union européenne à l'exception du Danemark, qui n'a pas participé à l'adoption de la directive, conformément aux articles 1er et 2 du protocole sur la position du Danemark, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne (TFUE). Conformément à l'article 3 du protocole 21 sur la position du Royaume-Uni et de l'Irlande, ces deux pays ont pris part à l'adoption de la directive et sont liées par celle-ci.

[4] Tous les articles mentionnés font référence à ceux de la directive, sauf mention contraire.

«convention de Budapest»), excepté le fait que la définition de la directive inclut également de manière explicite les données informatiques elles-mêmes;
- les «données informatiques» à l'article 2, point b). La définition suit celle de l'article 1, point b, de la convention de Budapest, en faisant référence à un système d'information plutôt qu'à un système informatique;
- une «personne morale» à l'article 2, point c). La définition vise à garantir la responsabilité des personnes physiques et morales, tout en excluant les États, les entités publiques et les organisations internationales relevant du droit public;
- «sans droit» à l'article 2, point d). La définition porte sur un principe général du droit pénal et vise à éviter qu'une personne agissant comme la loi nationale l'y autorise ou avec l'autorisation du propriétaire du système d'information ou d'un autre titulaire de droits sur celui-ci ou une partie de celui-ci ne voie sa responsabilité pénale engagée.

Des infractions pénales spécifiques sont définies, à savoir:
- l'accès illégal à des systèmes d'information en tant que tel (article 3);
- l'atteinte illégale à l'intégrité d'un système (article 4), qui inclut tout accès illégal à un système d'information entraînant une perturbation grave ou une interruption de son fonctionnement;
- l'atteinte illégale à l'intégrité des données (article 5), qui concerne toute atteinte illégale à des données informatiques qui compromet leur intégrité ou leur disponibilité;
- l'interception illégale (article 6) de transmissions non publiques de données informatiques et d'émissions électromagnétiques provenant d'un système d'information transportant de telles données;
- la fourniture illégale d'outils utilisés pour commettre les infractions susmentionnées (article 7). Dans ce contexte, il peut s'agir de programmes informatiques, de mots de passe ou de toutes autres données permettant d'accéder à un système d'information.

De plus, la directive **étend la responsabilité pénale** au fait, pour des personnes physiques ou morales, d'inciter à commettre les infractions susmentionnées, d'y participer ou de s'en rendre complice, ainsi qu'à la tentative de les commettre (article 8). Tandis que le fait d'inciter, de participer ou de se rendre complice concerne l'ensemble des infractions mentionnées aux articles 3 à 7, la tentative ne vise que les articles 4 et 5.

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

- de manière générale, une peine d'emprisonnement maximale d'au moins deux ans est prévue pour toutes les infractions, à l'exception de celles relevant de l'article 8 (article 9, paragraphe 2);
- une peine d'emprisonnement maximale d'au moins trois ans s'applique aux infractions visées aux articles 4 et 5 lorsqu'un nombre important de systèmes d'information est atteint (on parle généralement d'infractions par réseau zombie; article 9, paragraphe 3);
- une peine d'emprisonnement maximale d'au moins cinq ans est requise pour les infractions visées aux articles 4 et 5 si elles sont commises par une organisation criminelle [article 9, paragraphe 4, point a)], causent un préjudice grave [article 9, paragraphe 4, point b)] ou sont commises contre un système d'information d'une infrastructure critique [article 9, paragraphe 4, point c)];

- lorsqu'une infraction visée aux articles 4 et 5 est commise dans le cadre de l'utilisation abusive des données à caractère personnel d'une autre personne, les États membres doivent veiller à ce que cela puisse être considéré comme une circonstance aggravante, à moins que cette circonstance ne soit déjà couverte par une autre infraction (article 9, paragraphe 5).

Les articles suivants établissent les conditions minimales de la **responsabilité des personnes morales** (article 10) et fournissent une liste indicative des sanctions qui peuvent être appliquées à celles-ci (article 11).

Reconnaissant que les infractions susmentionnées peuvent être commises (au sens d'«exécutées») à l'endroit où agit effectivement l'auteur tandis que leurs effets sur les systèmes d'information visés peuvent se produire à un autre endroit, l'article 12 prévoit l'obligation d'établir la **compétence** en opérant une distinction entre les éléments suivants:

- l'endroit où l'auteur se trouve physiquement lorsque l'infraction est commise;
- l'endroit où se trouve le système d'information visé;
- la nationalité de l'auteur;
- sa résidence habituelle, et
- l'endroit où est établie la personne morale pour le compte de laquelle l'infraction a été commise.

En ce qui concerne l'échange d'informations, l'article 13, paragraphe 1, 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.

De plus, les États membres doivent prendre les mesures nécessaires afin de **faciliter la notification** des infractions susmentionnées aux autorités nationales compétentes (article 13, paragraphe 3) et de collecter et communiquer une quantité minimale de **données statistiques** portant sur ces infractions (article 14).

1.2 Objet et méthodologie du rapport

L'article 16 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 4 septembre 2015 et de les communiquer à la Commission.

Le présent rapport répond à l'obligation visée à l'article 17 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 dispositions nécessaires afin de se conformer à la directive. Ce rapport vise donc à fournir un aperçu concis mais instructif 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, 22 États membres avaient notifié à la Commission l'achèvement de la transposition de la directive. En novembre 2015, la Commission a engagé des procédures d'infraction pour non-communication de mesures nationales de transposition à l'encontre des cinq autres États membres: BE, BG, EL, IE et SI[5]. Au 31 mai 2017, les procédures d'infraction pour non-communication de mesures nationales de transposition à l'encontre de BE, BG et IE étaient toujours en cours[6].

La description et l'analyse contenues dans le présent rapport sont basées sur les informations communiquées par les États membres au plus tard le 31 mai 2017[7]. 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 avéré nécessaire et approprié afin de recevoir 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 et d'autres dispositions non notifiées à la Commission ou que des développements législatifs et non législatifs futurs 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 (article 2 de la directive)

L'article 2 de la directive fournit une définition juridique des termes «système d'information» [point a)], «données informatiques» [point b)], «personne morale» [point c)] et «sans droit» [point d)]. Seuls CY et UK (Gibraltar) ont introduit une législation couvrant tous les aspects des définitions énumérées ci-dessus. Plus précisément:

a) Système d'information

La définition de la directive s'appuie sur la définition du terme «système informatique» énoncée à l'article 1, point a, de la convention de Budapest, en ajoutant les données informatiques elles-mêmes en tant que partie du système d'information. CY, EL, IE, FI, HR, MT, PT et UK (Gibraltar) ont introduit des dispositions législatives contenant la définition d'un système d'information, tandis que les informations fournies par DE, ES, FR, LU, LV, PL, SE et SK n'étaient pas concluantes. En ce qui concerne les autres États membres, c'est-à-dire AT, BE, BG, CZ, EE, HU, IT, LT, NL, RO, SI et UK (sauf Gibraltar), leurs définitions juridiques respectives ne mentionnent pas de manière spécifique les «données informatiques». Cela implique une référence à l'article 1, point a, de la convention de Budapest, avec une portée identique de la définition d'un système informatique.

[5] Les États-membres sont désignés par leur sigle dans le présent document, conformément à: http://publications.europa.eu/code/fr/fr-5000600.htm.

[6] Des informations concernant les décisions prises par la Commission en matière de procédures d'infraction sont disponibles à l'adresse suivante: http://ec.europa.eu/atwork/applying-eu-law/infringements-proceedings/infringement_decisions/?lang_code=fr.

[7] IE a notifié la transposition complète de la directive le 31 mai 2017.

b) Données informatiques
Le terme «données informatiques» est prévu par la législation de AT, BG, CY, CZ, DE, EE, EL, IE, FI, HR, LT, MT, NL, PT, RO et UK (Gibraltar), tandis que les informations fournies par ES, FR, IT, LU, LV, PL, SE, SK et UK (sauf Gibraltar) n'étaient pas concluantes. Cependant, dans le cas de SE, cette définition serait redondante en raison de l'organisation spécifique des articles de référence. En ce qui concerne les autres États membres, HU fait référence à la définition des données informatiques uniquement pour les infractions décrites aux articles 4 et 5 de la directive, tandis que BE et SI n'ont pas inclus dans leur définition des données informatiques le passage suivant: «programme de nature à faire en sorte qu'un système d'information exécute une fonction».

c) Personne morale
À l'exception de LU, qui n'a pas fourni d'informations concluantes concernant la transposition de l'article 2, point c), la transposition de la définition d'une personne morale» n'a pas causé de problèmes. Cela s'explique par le fait que, de manière générale, elle se trouve déjà dans les dispositions du droit civil ou commercial des États membres. Seules les mesures adoptées par CY pour transposer la directive contiennent une disposition spécifique.

d) Sans droit
En ce qui concerne la définition du terme «sans droit» qui figure à l'article 2, point d), seuls CY, IE, RO et UK (Gibraltar) ont notifié la transposition, ce qui signifie que 23 États membres n'ont adopté aucune mesure de transposition pour cette définition. Cependant, il y a lieu de souligner que l'on retrouve dans tous les États membres le principe général selon lequel aucune responsabilité pénale ne peut être engagée au titre d'une action si l'auteur de cette action dispose des droits correspondants.

2.2 Infractions pénales spécifiques (articles 3 à 7 de la directive)

a) Accès illégal à des systèmes d'information
L'article 3 de la directive, qui porte sur l'accès illégal à un système d'information, est couvert par la législation nationale de AT, CY, CZ, EL, ES, IE, FI, FR, LT, LU, NL, PL, PT, SE et SK.

En ce qui concerne tous les autres États membres, c'est-à-dire BE, BG, DE, EE, HR, HU, IT, LV, MT, RO, SI et UK, les descriptions nationales respectives de cette infraction pénale n'opèrent pas de distinction entre le fait d'accéder à l'ensemble du système d'information ou de n'accéder qu'à une partie de celui-ci, bien que la directive le prévoie de manière explicite. De plus, la transposition de DE ne couvre pas le simple accès au matériel informatique, tandis que AT et LU prévoient des exigences supplémentaires concernant l'existence d'une intention particulière (intention d'acquérir des connaissances, de causer un préjudice ou intention frauduleuse) et que LV prévoit une exigence supplémentaire concernant la cause d'un préjudice grave. Dans le cas de BE, BG, FR, HR, LU, MT, PT, RO, SI et UK, la portée des dispositions nationales est plus large que celle de la directive en ce que celles-ci ne nécessitent pas la violation d'une mesure de sécurité pour établir la responsabilité pénale. Les autres États membres indiquent littéralement que l'infraction doit être commise en violant une mesure de sécurité (CY, EL et SK), ou utilisent une terminologie similaire afin de décrire cet aspect (AT, CZ, DE, EE, ES, FI, HU, IT, LT, LV, NL, PL et SE).

b) Atteinte illégale à l'intégrité d'un système
L'article 4 de la directive porte sur l'atteinte illégale à l'intégrité d'un système. La directive énumère huit actes possibles (introduire, transmettre, endommager, effacer, détériorer, altérer, supprimer ou rendre inaccessibles des données informatiques) et deux résultats possibles de

ces actes (provoquer une perturbation grave ou une interruption du fonctionnement d'un système d'information). BE, CY, CZ, EL, IE, FR, HR, LU, MT, PT, SE et UK (sauf Gibraltar) ont introduit les mesures législatives correspondantes. BG ne fait référence qu'à l'introduction d'un virus, tandis que les autres États membres (AT, DE, EE, ES, HU, IT, LV, NL, PL, RO, SI, SK et UK) omettent de mentionner de manière spécifique jusqu'à quatre des actes possibles. Dans ce contexte, il convient d'observer que la plupart des problèmes sont liés aux termes «détériorant» (absent dans 8 cas) et «rendant inaccessibles» (absent dans 9 cas).

c) Atteinte illégale à l'intégrité des données

L'article 5 de la directive concerne l'atteinte illégale à l'intégrité des données et énumère les six actes possibles suivants: effacer, endommager, détériorer, altérer, supprimer ou rendre inaccessibles des données informatiques. CY, EL, IE et MT ont transposé la disposition littéralement; BE, CZ, LT, PT et SE ont utilisé des termes plus génériques afin de couvrir l'ensemble des actes possibles. Les mesures de transposition de tous les autres États membres ne couvrent pas toutes les possibilités mais font seulement référence à cinq d'entre elles (FI et SK) ou moins (AT, BG, DE, EE, FR, HR, HU, IT, LU, NL, PL, RO, SI et UK). La plupart des problèmes sont liés aux termes «endommager» (absent 8 fois), «détériorer» (absent 13 fois), «supprimer» (absent 11 fois) et «rendre inaccessibles des données informatiques» (absent 13 fois). En plus de la formulation de la directive, FI exige l'existence d'une «intention de causer un préjudice ou une perte financière» pour engager la responsabilité pénale, tandis que LT et LV exigent que «l'acte entraîne des dommages conséquents ou un préjudice grave».

d) Interception illégale

L'article 6 porte sur l'interception illégale et vise les transmissions non publiques de données informatiques et les émissions électromagnétiques provenant d'un système d'information transportant de telles données. CY, CZ, DE, ES, IE, FI, HR, LV, MT, RO, SE, SK et UK (Gibraltar) ont introduit une législation qui couvre l'article 6 dans son intégralité. Alors que la directive concerne l'interception de données informatiques en général, celle-ci est, dans certains États membres, limitée aux messages (AT et BG), à l'observation d'une personne (EE) ou à la correspondance (FR et HU). Par ailleurs, les mesures de transposition des États membres suivants ne couvrent par l'interception des émissions électromagnétiques: BE, BG, EE, FR, HU, IT, LT, LU, NL, PL, PT, SI et UK (sauf Gibraltar). De plus, certains États membres exigent une intention particulière (acquérir des connaissances, réaliser un profit ou causer un préjudice, voir AT, EL, HU) ou des actes supplémentaires spécifiques (par exemple, l'enregistrement ou le fait de prendre connaissance du contenu intercepté, voir BG et HU).

e) Outils utilisés pour commettre les infractions

L'article 7 érige en infractions pénales un certain nombre d'actes concernant les outils, tels que les programmes informatiques ou les codes d'accès, qui sont utilisés pour commettre les infractions mentionnées aux articles 3 à 6: la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition de ces outils. AT, BE, CY, DE, EL, IE et SK ont introduit une législation nationale correspondante. Certains États membres ne couvrent pas toutes les infractions mentionnées (EE, IT, MT, PL et SI). Certains ne mentionnent pas l'auteur de l'infraction au titre de l'article 7 comme étant une personne différente de l'auteur des infractions mentionnées aux articles 3 à 6 (CZ et SI). Certains États membres exigent une intention spécifique (causer un préjudice ou agir de manière frauduleuse, voir FI, IT et LU), un résultat spécifique comme la violation de la confidentialité (BG), ou au minimum un certain degré de préparation des infractions mentionnées (SE). Enfin, il existe des différences entre l'article 7 et les mesures nationales en raison de l'absence de transposition de tous les actes possibles énumérés. C'est le cas pour BG, CZ, EE, ES, FR,

HR, HU, IT, LT, LU, LV, PL, PT, RO, SI et UK. Parmi ces derniers, la législation de LU mentionne de manière spécifique cinq des six actes possibles énumérés dans la directive, tandis que les autres États membres ne font référence qu'à quatre de ces actes ou moins.

ES est le seul à avoir transposé la notion d'obtention pour utilisation.

2.3 Règles générales relatives aux infractions concernées (articles 8 à 12 de la directive)

a) Incitation, participation et complicité
L'article 8, paragraphe 1, fait obligation aux États membres de veiller à ériger en infraction pénale punissable le fait d'inciter à commettre l'une des infractions visées aux articles 3 à 7, d'y participer ou de s'en rendre complice. Tous les États membres ont transposé cette disposition.

b) Tentative
Conformément à l'article 8, paragraphe 2, la tentative de commettre les infractions visées aux articles 4 et 5 doit être érigée en infraction pénale punissable. PT ne couvre pas tous les types de tentative de commission des infractions visées à l'article 4 et SE ne prévoit pas de responsabilité pénale pour la tentative de commission de l'infraction de «violation du secret des communications», mais tous les autres États membres ont adopté une législation qui transpose cette disposition.

c) Sanctions

aa) Dispositions générales
L'article 9, paragraphe 1, oblige les États membres, de manière générale, à prévoir des sanctions pénales effectives, proportionnées et dissuasives pour les infractions relevant de la directive. Bien que la plupart des États membres s'y soient conformés, AT, BE, BG, IT, PT, SE et SI ne respectent pas dans tous les cas le niveau minimal des peines maximales fixé à l'article 9, paragraphe 2 (voir section 1.1 ci-dessus). Cela a une incidence sur la transposition de l'article 9, paragraphe 1, car il est possible de conclure que les exigences minimales de l'article 9, paragraphe 2, constituent le minimum requis permettant de garantir l'existence de sanctions pénales effectives, proportionnées et dissuasives.

bb) Niveau minimal général de la peine maximale
Conformément à l'article 9, paragraphe 2, le niveau minimal de la peine maximale pour les infractions ordinaires mentionnées aux articles 3 à 7 est une peine d'emprisonnement d'au moins deux ans. La plupart des États membres respectent cette disposition. Seuls six États membres s'en écartent: AT (peine maximale d'emprisonnement de six mois), BG (peine maximale d'emprisonnement d'un an pour toutes les infractions à l'exception de l'interception illégale), IT [peine maximale d'emprisonnement d'un an pour l'infraction visée à l'article 7, point b)], PT (peine maximale d'emprisonnement d'un an pour l'infraction visée à l'article 3), SE (peine maximale d'emprisonnement d'un an pour l'infraction consistant à «causer un préjudice») et SI (peine maximale d'emprisonnement d'un an pour les infractions visées aux articles 3, 6 et 7). Dans le cas de BE, le niveau minimal de la peine maximale prévue pour les articles 3, 6 et 7 n'est atteint que lorsque les infractions sont commises avec une intention frauduleuse.

cc) Un nombre important de systèmes d'information est atteint
L'article 9, paragraphe 3, relève le niveau minimal de la peine maximale à trois ans d'emprisonnement lorsqu'un nombre important de systèmes d'information est atteint par une infraction visée aux articles 4 et 5. De manière générale, les États membres ont introduit la

législation correspondante; DE mentionne uniquement les systèmes d'information «revêtant une importance considérable pour un autre système», FI exige qu'une évaluation de l'infraction «dans son ensemble» soit réalisée pour appliquer la sanction aggravée et LV ne fait pas référence à un nombre important de systèmes d'information (ou à une formulation similaire), mais uniquement au fait de causer «un préjudice important». Les informations fournies par BG et SI n'étaient pas concluantes.

dd) Organisations criminelles

Conformément à l'article 9, paragraphe 4, point a), les infractions visées aux articles 4 et 5 sont passibles d'une peine d'emprisonnement maximale d'au moins cinq ans lorsqu'elles sont commises par une organisation criminelle telle que définie dans la décision-cadre 2008/841/JAI.

Une fois encore, la plupart des États membres respectent la disposition de l'article 9, paragraphe 4, point a). En vertu du droit pénal de LU et SI, les dispositions concernant les infractions commises par une organisation criminelle ne couvrent pas la cybercriminalité. La législation de BE prévoit une peine maximale de seulement trois ans d'emprisonnement pour les infractions visées à l'article 5, la législation de DE n'inclut pas les personnes physiques en tant que victimes de ces infractions, la législation de FI exige qu'une évaluation supplémentaire de l'infraction «dans son ensemble» soit réalisée et la législation de SE prévoit une peine maximale de quatre ans d'emprisonnement pour l'infraction consistant à «causer un préjudice important».

ee) Préjudice grave causé

Conformément à l'article 9, paragraphe 4, point b), les infractions visées aux articles 4 et 5 sont passibles d'une peine d'emprisonnement maximale d'au moins cinq ans lorsqu'elles causent un préjudice grave. Bien qu'il n'existe aucune définition de ce qu'il convient de considérer comme un préjudice grave, tous les États membres à l'exception de BG, DE, FI, HU, LU et SE ont introduit une législation correspondant à la directive. Les informations fournies par HU n'étaient pas concluantes. BG n'atteint pas le niveau minimal d'une peine maximale de cinq ans d'emprisonnement, tandis que LU renvoie à une disposition générale sanctionnant le fait de causer un préjudice grave, qui ne couvre pas la cybercriminalité. Il existe des différences mineures en DE (les personnes physiques ne sont pas couvertes comme victimes des infractions), en FI (la peine aggravée nécessite la réalisation d'une évaluation supplémentaire de l'infraction «dans son ensemble») et en SE (peine d'emprisonnement maximale de quatre ans pour le fait de «causer un préjudice important»).

ff) Systèmes d'information d'infrastructure critique

L'implication de systèmes d'information d'infrastructures critiques dans les infractions visées aux articles 4 et 5 entraîne également une peine maximale d'emprisonnement d'au moins cinq ans, conformément à l'article 9, paragraphe 4, point c).

La plupart des États membres respectent cette disposition, mais BG n'a fourni aucune information spécifique relative à sa transposition. BE a établi une peine d'emprisonnement maximale de trois ans pour les infractions visées à l'article 5. DE n'inclut pas les personnes physiques en tant que victimes. FI impose qu'une évaluation supplémentaire de l'infraction «dans son ensemble» soit réalisée, IT exige qu'une «destruction» soit effectivement causée, PT prévoit que l'attaque doit se produire «de manière sévère et durable» et ne fait pas référence à l'article 5 et SE ne respecte les exigences de la directive qu'en ce qui concerne l'infraction de «sabotage caractérisé».

gg) Usurpation d'identité et autres infractions liées à l'identité

L'article 9, paragraphe 5, impose aux États membres de veiller à ce que, lorsque les infractions visées aux articles 4 et 5 sont commises par l'utilisation abusive des données à caractère personnel d'une autre personne, en vue de gagner la confiance d'une tierce partie, causant ainsi un préjudice au propriétaire légitime de l'identité, ces éléments puissent être considérés comme des circonstances aggravantes, à moins que ces circonstances ne soient déjà couvertes par une autre infraction punissable en vertu du droit national. L'importante marge d'appréciation a conduit à une vaste gamme de mesures de transposition parmi les États membres. BE et EL n'ont notifié aucune transposition et il n'existe pas de disposition spécifique dans la législation pénale de CZ. L'option des circonstances aggravantes a été retenue par AT, CY, ES, IE, MT, PT et SE (ce dernier État membre faisant référence à la circonstance d'une «planification particulière»), tandis que tous les autres États membres renvoient à des dispositions additionnelles pour l'infraction pénale spécifique. Parmi les États membres qui font référence à des dispositions spécifiques, on peut observer les problèmes de transposition suivants: BG et NL exigent une intention particulière («procurer un avantage» et «en vue de dissimuler ou d'utiliser abusivement l'identité»), DE fait uniquement référence aux «données à caractère personnel qui ne sont pas généralement accessibles», FR fait uniquement référence au nom d'une personne et pas aux autres données à caractère personnel, LV exige qu'un «préjudice important» ait été causé, RO prévoit uniquement l'utilisation d'«un document» et exige le recours à la tromperie.

d) Responsabilité des personnes morales

aa) En général

L'article 10, paragraphe 1, exige que la responsabilité des personnes morales soit établie pour les infractions visées aux articles 3 à 8 si l'auteur a) exerce un pouvoir de représentation de la personne morale, b) dispose d'une autorité pour prendre des décisions au nom de la personne morale ou c) dispose d'une autorité pour exercer un contrôle au sein de la personne morale. Tous les États membres ont introduit une législation correspondant à cet article, avec seulement les quelques problèmes suivants: BG ne couvre pas l'infraction visée à l'article 6 et HR ne mentionne pas le cas d'un auteur qui disposerait d'une l'autorité pour exercer un contrôle au sein de la personne morale [article 10, paragraphe 1, point c)].

bb) En raison d'une absence de surveillance ou de contrôle

L'article 10, paragraphe 2, fait obligation aux États membres de prévoir la responsabilité des personnes morales lorsqu'une infraction visée aux articles 3 à 8 a été rendue possible par l'absence de surveillance ou de contrôle d'une personne visée à l'article 10, paragraphe 1. Bien que la plupart des États membres se conforment à cette disposition, les informations fournies par LU n'étaient pas concluantes et BG ne mentionne pas la commission d'une infraction visée à l'article 6.

e) Sanctions à l'encontre des personnes morales

aa) Sanctions obligatoires

L'article 11, paragraphe 1, de la directive impose aux États membres de prévoir des amendes pénales ou non pénales à titre de sanctions effectives, proportionnées et dissuasives pour les personnes morales. Tous les États membres ont notifié des mesures nationales conformes, à l'exception de IE et UK. Dans ces deux pays, le montant maximal des amendes éventuelles n'est toujours pas déterminé en raison de l'absence de dispositions législatives concrètes. Par conséquent, il n'est pas possible de procéder à l'appréciation du caractère effectif, proportionné ou dissuasif des amendes respectives.

bb) Sanctions optionnelles

L'article 11, paragraphe 1, poursuit en énumérant des options de sanctions supplémentaires envisageables pour les personnes morales, à savoir: l'exclusion du bénéfice d'un avantage ou d'une aide publics (retenue par CY, CZ, EL, ES, HR, HU, LU, MT, PL, PT et SK), l'interdiction temporaire ou définitive d'exercer une activité commerciale (AT, BE, CY, CZ, EL, ES, FR, HR, HU, IT, LT, LV, MT, PL, PT, RO, SE, SI et SK), le placement sous surveillance judiciaire (CY, ES, FR, MT, PT et RO), une mesure judiciaire de dissolution (CY, CZ, EL, ES, FR, HR, HU, LT, LU, LV, MT, PT, RO, SI et SK) et la fermeture temporaire ou définitive d'établissements ayant servi à commettre l'infraction (BE, CY, WS, FR, LT, MT, PT et RO). BG, DE, EE, IE, FI, NL et UK n'ont retenu aucune de ces options.

cc) Sanctions pour omission

Conformément à l'article 11, paragraphe 2, les États membres doivent veiller à ce que des sanctions effectives, proportionnées et dissuasives soient applicables aux personnes morales responsables d'une infraction par omission telle que visée à l'article 10, paragraphe 2. Les informations fournies par LU n'étaient pas concluantes. Tous les autres États membres, à l'exception de IE et UK, ont prévu les dispositions législatives correspondantes. En ce qui concerne IE et UK, le même problème s'est posé que pour l'article 11, paragraphe 1, [voir point aa) ci-dessus].

f) Compétence

aa) Règles de compétence nécessaires

L'article 12, paragraphes 2 et 3, de la directive exige que les États membres établissent leur compétence pour les infractions visées aux articles 3 à 8 lorsque l'infraction a été commise en tout ou en partie sur leur territoire –parce que l'auteur était présent physiquement sur place lors de la commission de l'infraction ou parce que le système d'information visé était situé sur le territoire de l'État membre – ou lorsque l'infraction a été commise à l'étranger par un ressortissant de l'État membre. La plupart des États membres ont introduit la législation nationale correspondante; la législation d'IT n'établit pas de compétence pour les ressortissants se trouvant à l'étranger pour les infractions de base, les législations de LV et de SI renvoient à des dispositions peu claires en ce qui concerne l'aspect territorial, la compétence de MT pour une commission partielle sur son territoire n'est pas claire et UK fait référence à un système informatique et non à un système d'information.

bb) Autres règles de compétence

L'article 12, paragraphe 3, prévoit que lorsqu'un État membre établit sa compétence dans les cas où l'auteur de l'infraction réside habituellement sur son territoire (option retenue par AT, CY, CZ, IE, FI, HR, LT, LV, NL, SE et SK) ou si l'infraction a été commise pour le compte d'une personne morale établie sur son territoire (CY, CZ, LV, PT, RO et SK), il doit en informer la Commission.

2.4 Questions d'ordre opérationnel (articles 13 et 14 de la directive)

a) Disposition relative aux points de contact nationaux opérationnels

L'article 13, paragraphe 1, invite les États membres à établir des points de contact nationaux opérationnels en vue d'échanger des informations relatives aux infractions visées aux articles 3 à 8. Sur la base de cette disposition, les États membres doivent garantir que des procédures sont en place pour permettre à l'autorité compétente de répondre dans un délai de huit heures à compter de la réception de toute demande urgente d'assistance. D'après les informations notifiées, la plupart des États membres ont mis en place les infrastructures nécessaires. IE et RO ont indiqué que leurs points de contact respectifs ne sont disponibles que quelques heures chaque jour, ce qui ne permet pas à l'autorité de réagir dans un délai de

huit heures à compter de la réception d'une demande dans tous les cas envisageables. Plusieurs États membres ont indiqué qu'ils se servent de réseaux existants de points de contact opérationnels, établis grâce au réseau G7 ou en vertu de la convention de Budapest sur la cybercriminalité du Conseil de l'Europe.

b) Informations relatives aux points de contact nationaux opérationnels établis
Conformément à l'article 13, paragraphe 2, les États membres doivent fournir les coordonnées de leur point de contact à la Commission, qui les transmet aux autres États membres. Tous les États membres ont fourni les informations nécessaires.

c) Canaux de communication
L'article 13, paragraphe 3, impose aux États membres de faire en sorte que des canaux de communication appropriés soient mis à disposition afin de faciliter la notification aux autorités nationales compétentes des infractions visées aux articles 3 à 6. Les informations fournies par HR, IT, IE et PT n'étaient pas concluantes. Parmi les autres États membres, il semble qu'il existe différentes approches de mise en œuvre des canaux de communication. La plupart des États membres (BE, BG, CY, CZ, DE, EE, EL, FI, FR, HR, HU, IT, LT, LV, MT, NL, PL, PT, RO, SE, SI, SK et UK) ont notifié des mesures qui prévoient des canaux visant à faciliter la notification d'une infraction par la personne ou l'organisation à l'origine de la notification, par exemple la victime d'une cyberattaque (les canaux réels de communication demeurant peu clairs pour LV). Cependant, d'autres États membres (AT, ES et LU) ont fourni des informations identiques concernant la mise en œuvre de l'article 13, paragraphes 1 et 2, desquelles il ressort que leurs mesures tendent principalement à faciliter la communication entre les autorités.

d) Collecte de données statistiques
Conformément à l'article 14, paragraphes 1 et 2, les États membres doivent veiller à mettre en place un système d'enregistrement, de production et de communication de statistiques, portant au minimum sur le nombre d'infractions visées aux articles 3 à 7 enregistrées par les États membres et sur le nombre de personnes poursuivies et condamnées pour ces infractions. D'après les notifications reçues, la plupart des États membres ont mis en place des mesures législatives et administratives afin de garantir la collecte des informations, généralement au moyen d'un système électronique national général. Les informations fournies par plusieurs États membres n'étaient pas concluantes [EL, IE, UK (Gibraltar, Irlande du Nord et Écosse)]. Cette situation s'explique notamment par le fait que les informations concernant les infractions spécifiques visées par la directive ne peuvent pas être collectées séparément (BE, DE et SE) ou que les informations collectées peuvent ne pas couvrir l'ensemble des infractions visées par la directive (RO).

e) Transmission des statistiques à la Commission
L'article 14, paragraphe 3, invite les États membres à transmettre leurs statistiques respectives à la Commission. Tous les États membres qui ont notifié des mesures, à l'exception de UK (Gibraltar, Irlande du Nord et Écosse) et HU, ont confirmé avoir mis en œuvre des mesures juridiques et/ou administratives afin d'assurer le respect de cette obligation. Les informations concernant EL, ES, LU et SI n'étaient pas concluantes.

3. Conclusions et étapes suivantes

La directive a permis d'accomplir des progrès substantiels en matière de criminalisation des cyberattaques 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. Jusqu'à présent, l'analyse suggère que certaines des principales améliorations à mettre en œuvre par les États membres concernent l'utilisation des définitions (article 2), qui a un effet sur la portée des infractions définies par le droit national sur la base de la directive. De plus, il semblerait que certains États membres aient rencontré des difficultés pour inclure l'ensemble des possibilités qui caractérisent les actions liées aux infractions (articles 3 à 7) et pour prévoir des normes communes en matière de sanctions pour les cyberattaques (article 9). D'autres problèmes semblent liés à la mise en œuvre des dispositions administratives concernant les canaux de communication appropriés (article 13, paragraphe 3) ainsi qu'au suivi et aux statistiques concernant les infractions relevant de la directive (article 14).

La Commission continuera de soutenir les États membres dans leur mise en œuvre de la directive. En ce qui concerne la contribution potentielle à la coopération transfrontière, il s'agit notamment des dispositions opérationnelles de la directive relatives à l'échange d'informations (article 13, paragraphes 1 et 2), aux canaux de communication (article 13, paragraphe 3) et au suivi et aux statistiques (article 14). À cet égard, la Commission fournira aux États membres des occasions supplémentaires de recenser et d'échanger leurs bonnes pratiques au cours du second semestre 2017.

Pour le moment, la Commission ne voit pas la nécessité de proposer des modifications de la directive. Dans ce contexte, et afin de rendre plus aisées les enquêtes criminelles relatives aux attaques contre les systèmes d'information, aux formes de criminalité facilitées par les technologies de l'information et à tous les autres types de criminalité, la Commission envisage des mesures visant à améliorer l'accès transfrontière aux preuves électroniques dans le cadre des enquêtes criminelles, notamment en proposant des mesures législatives au début de 2018[8]. La Commission étudie également le rôle que joue le chiffrement dans les enquêtes criminelles et présentera ses conclusions sur le sujet d'ici octobre 2017[9].

La Commission est résolue à ce que la transposition soit finalisée dans l'ensemble de l'Union et à ce que les dispositions soient correctement appliquées. Cela implique notamment de s'assurer que les mesures nationales sont conformes aux dispositions correspondantes de la directive. Le cas échéant, la Commission fera usage de ses pouvoirs d'exécution en vertu des traités au moyen de procédures d'infraction.

[8] Analyse d'impact initiale relative à l'amélioration de l'accès transfrontière aux preuves électroniques, du 4 août 2017, disponible à l'adresse ec.europa.eu.

[9] Communication sur le huitième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective, COM(2017) 354 final.