P7_TA-PROV(2013)0321

Attaques visant les systèmes d'information ***I

Résolution législative du Parlement européen du 4 juillet 2013 sur la proposition de directive du Parlement européen et du Conseil relative aux attaques visant les systèmes d'information et abrogeant la décision-cadre 2005/222/JAI du Conseil (COM(2010)0517 – C7-0293/2010 – 2010/0273(COD))

(Procédure législative ordinaire: première lecture)

Le Parlement européen,

– vu la proposition de la Commission au Parlement européen et au Conseil (COM(2010)0517),

– vu l'article 294, paragraphe 2, et l'article 83, paragraphe 1, du traité sur le fonctionnement de l'Union européenne, conformément auxquels la proposition lui a été présentée par la Commission (C7-0293/2010),

– vu l'article 294, paragraphe 3, du traité sur le fonctionnement de l'Union européenne,

– vu l'avis du Comité économique et social européen du 4 mai 2011[1],

– vu l'engagement pris par le représentant du Conseil, par lettre du 21 juin 2013, d'approuver la position du Parlement européen, conformément à l'article 294, paragraphe 4, du traité sur le fonctionnement de l'Union européenne,

– vu l'article 55 de son règlement,

– vu le rapport de la commission des libertés civiles, de la justice et des affaires intérieures et les avis de la commission des affaires étrangères et de la commission de l'industrie, de la recherche et de l'énergie (A7-0224/2013),

1. arrête la position en première lecture figurant ci-après;

2. demande à la Commission de le saisir à nouveau, si elle entend modifier de manière substantielle sa proposition ou la remplacer par un autre texte;

3. charge son Président de transmettre la position du Parlement au Conseil et à la Commission ainsi qu'aux parlements nationaux.

[1] JO C 218 du 23.7.2011, p. 130.

P7_TC1-COD(2010)0273

Position du Parlement européen arrêtée en première lecture le 4 juillet 2013 en vue de l'adoption de la directive 2013/.../UE du Parlement européen et du Conseil relative aux attaques contre les systèmes d'information et *remplaçant* la décision-cadre 2005/222/JAI du Conseil

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

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

vu la proposition de la Commission européenne,

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

vu l'avis du Comité économique et social européen[1],

statuant conformément à la procédure législative ordinaire[2],

---

1 ***JO C 218 du 23.7.2011, p. 130.***

2 Position du Parlement européen du 4 juillet 2013.

considérant ce qui suit:

(1) La présente directive a pour objectif de rapprocher ***le droit pénal*** des États membres dans le domaine des attaques contre les systèmes d'information ***en fixant des règles minimales concernant la définition des infractions pénales et les sanctions applicables, et de*** renforcer la coopération entre ▌ les autorités compétentes, notamment la police et les autres services spécialisés chargés de l'application de la loi dans les États membres, ***ainsi que les agences et organes spécialisés compétents de l'Union, tels qu'Eurojust, Europol et son Centre européen de lutte contre la cybercriminalité et l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA).***

(2) Les systèmes d'information représentent un élément essentiel de l'interaction politique, sociale et économique au sein de l'Union. La société est très dépendante de ce type de systèmes et ce phénomène va croissant. Le bon fonctionnement et la sécurité de ces systèmes au sein de l'Union sont fondamentaux pour le développement du marché intérieur et d'une économie compétitive et innovante. Le fait de garantir un niveau de protection approprié des systèmes d'information devrait faire partie d'un cadre global de mesures de prévention efficaces accompagnant les réponses pénales à la cybercriminalité.

(3) Les attaques contre les systèmes d'information, et en particulier celles ***liées*** à la criminalité organisée, constituent une menace croissante ***au sein de l'Union et à l'échelle mondiale***, et l'éventualité d'attaques terroristes ou politiques contre les systèmes d'information qui font partie de l'infrastructure critique des États membres et de l'Union suscite de plus en plus d'inquiétude. Cette situation menace la réalisation d'une société de l'information plus sûre et d'un espace de liberté, de sécurité et de justice, et appelle donc une réaction au niveau de l'Union ***ainsi qu'une amélioration de la coopération et de la coordination au niveau international.***

(4) Il existe plusieurs infrastructures critiques dans l'Union, dont l'arrêt ou la destruction aurait un impact transfrontalier significatif. Compte tenu de la nécessité de renforcer la capacité de protection des infrastructures critiques au sein de l'Union, il est devenu manifeste que les mesures de lutte contre les cyberattaques devraient s'accompagner de sanctions pénales sévères, reflétant la gravité de ces attaques. Une infrastructure critique pourrait s'entendre comme un point, un système ou une partie de celui-ci, situé dans des États membres, qui est indispensable au maintien des fonctions vitales de la société, de la santé, de la sûreté, de la sécurité et du bien-être économique ou social des citoyens, comme les centrales électriques, les réseaux de transport et les réseaux publics, et dont l'arrêt ou la destruction aurait un impact significatif dans un État membre du fait de la défaillance de ces fonctions.

(5) On constate une tendance à la perpétration d'attaques à grande échelle de plus en plus dangereuses et récurrentes contre des systèmes d'information ***qui*** peuvent souvent être critiques pour les États membres ou pour certaines fonctions du secteur public ou privé. Parallèlement, des méthodes de plus en plus sophistiquées sont mises au point***, telles que la création et l'utilisation de "réseaux zombies", qui implique une infraction pénale en plusieurs stades, chaque stade pouvant à lui seul menacer gravement les intérêts publics. La présente directive vise, entre autres, à mettre en place des sanctions pénales en ce qui concerne la création de réseaux zombies, c'est-à-dire l'acte d'établir un contrôle à distance d'un nombre important d'ordinateurs en les contaminant au moyen de logiciels malveillants dans le cadre de cyberattaques ciblées. Une fois créé, le réseau d'ordinateurs contaminés qui constitue le réseau zombie peut être activé à l'insu des utilisateurs des ordinateurs dans le but de lancer une cyberattaque à grande échelle, qui est en général à même de causer un grave préjudice, comme indiqué dans la présente directive. Les États membres peuvent déterminer, en fonction de leur droit national et de leur pratique nationale, ce qui constitue un préjudice grave, comme le fait d'arrêter des services de réseau présentant un intérêt public important, ou de causer des coûts financiers majeurs ou la perte de données à caractère personnel ou d'informations sensibles.***

(6) ***Des cyberattaques à grande échelle sont susceptibles de provoquer des dommages économiques notables, tant du fait de l'interruption des systèmes d'information et des communications qu'en raison de la perte ou de l'altération d'informations confidentielles importantes d'un point de vue commercial ou d'autres données. Il y a lieu en particulier de veiller à sensibiliser les petites et moyennes entreprises innovantes aux menaces liées à ces attaques et à leur vulnérabilité à cet égard, en raison de leur dépendance accrue à l'égard du bon fonctionnement et de la disponibilité des systèmes d'information et de leurs ressources limitées en matière de sécurité de l'information.***

(7) Des définitions communes dans ce domaine sont importantes pour garantir une approche cohérente des États membres quant à l'application de la présente directive.

(8) Il est nécessaire d'adopter une approche commune en ce qui concerne les éléments constitutifs des infractions pénales en instituant des infractions communes d'accès illégal à un système d'information, d'atteinte illégale à l'intégrité d'un système, d'atteinte illégale à l'intégrité des données et d'interception illégale.

(9) ***L'interception comprend, sans que cette liste ne soit limitative, l'écoute, le contrôle ou la surveillance du contenu des communications et l'obtention du contenu des données, soit directement, au moyen de l'accès aux systèmes d'information et de leur utilisation, soit indirectement, au moyen de l'utilisation de dispositifs d'écoute électroniques ou de dispositifs d'écoute par des moyens techniques.***

(10) Les États membres devraient prévoir des sanctions en ce qui concerne les attaques contre les systèmes d'information. Ces sanctions devraient être effectives, proportionnées et dissuasives ***et devraient comprendre des peines d'emprisonnement et/ou des amendes.***

(11) La présente directive prévoit des sanctions pénales au moins dans les cas où les faits ne sont pas mineurs. Les États membres peuvent déterminer, en fonction du droit national et de la pratique nationale, ce qui constitue un fait mineur. On peut considérer qu'un fait est mineur, par exemple, lorsque les dommages causés par l'infraction et/ou le risque pour les intérêts publics ou privés, tels que le risque pour l'intégrité d'un système informatique ou de données informatiques, ou pour l'intégrité, les droits ou les autres intérêts d'une personne, sont peu importants ou de nature telle qu'il n'est pas nécessaire d'appliquer une sanction pénale dans les limites du seuil légal ou que la responsabilité pénale soit engagée.

(12) La détection et la notification des menaces et des risques liés aux cyberattaques, ainsi que de la vulnérabilité des systèmes d'information à cet égard, sont des éléments pertinents pour prévenir les cyberattaques et y répondre de manière efficace, et pour améliorer la sécurité des systèmes d'information. Prévoir des mesures incitant à notifier les failles en matière de sécurité pourrait y contribuer. Les États membres devraient s'efforcer de prévoir les possibilités de détecter et de notifier de manière légale des failles en matière de sécurité.

(13) Il y a lieu de prévoir des sanctions plus sévères lorsque l'attaque contre un système d'information est commise par une organisation criminelle, telle que définie dans la décision-cadre 2008/841/JAI du Conseil du 24 octobre 2008 relative à la lutte contre la criminalité organisée[1], lorsqu'une cyberattaque est menée à grande échelle, ***affectant ainsi un grand nombre de systèmes d'information, y compris lorsque l'attaque a pour objectif de créer un réseau zombie, ou lorsqu'une cyberattaque cause un préjudice grave, y compris lorsqu'elle est menée via un réseau zombie.*** Il y a également lieu de prévoir des sanctions plus sévères lorsqu'une attaque est menée ***contre une infrastructure critique des États membres ou de l'Union.***

(14) La mise en place de mesures efficaces contre l'usurpation d'identité et d'autres infractions liées à l'identité constitue un autre élément important d'une approche intégrée contre la cybercriminalité. La nécessité de mener une action au niveau de l'Union contre ce type de comportement criminel pourrait également être envisagée dans le cadre de l'évaluation de la nécessité de disposer d'un instrument horizontal global au niveau de l'Union.

(15) Dans ses conclusions des 27 et 28 novembre 2008, le Conseil a indiqué qu'il convenait que les États membres et la Commission définissent une nouvelle stratégie, en prenant en considération le contenu de la convention du Conseil de l'Europe de 2001 sur la cybercriminalité. Cette convention est le cadre juridique de référence pour la lutte contre la cybercriminalité, y compris les attaques contre les systèmes d'information. La présente directive s'en inspire. ***Il faudrait se donner pour priorité d'achever, le plus rapidement possible, le processus de ratification de cette convention par tous les États membres.***

---

[1] JO L 300 du 11.11.2008, p. 42.

(16) Compte tenu des différentes façons dont les attaques peuvent être menées et de l'évolution rapide des équipements et des logiciels, la présente directive ***fait référence*** à des outils qui peuvent être utilisés pour commettre les infractions prévues dans la présente directive. Ces outils pourraient comprendre des logiciels malveillants, notamment ***ceux qui sont capables*** de créer des réseaux zombies, utilisés pour lancer des cyberattaques. ***Même si cet outil est adapté ou particulièrement adapté pour commettre l'une des infractions prévues dans la présente directive, il se peut qu'il ait été produit à des fins légitimes. Dès lors qu'il faut éviter d'ériger en infractions la production et la commercialisation de ces outils à des fins légitimes, par exemple pour tester la fiabilité de produits relevant des technologies de l'information ou la sécurité des systèmes d'information, il faut, pour qu'il y ait infraction, outre une intention générale, une intention spécifique d'utiliser ces outils afin de commettre l'une ou plusieurs des infractions prévues dans la présente directive.***

(17) La présente directive n'impose pas de responsabilité pénale lorsque les critères objectifs constitutifs des infractions mentionnées dans la présente directive sont remplis, mais que les actes sont commis sans intention délictueuse, par exemple lorsqu'une personne ne sait pas que l'accès n'était pas autorisé ou dans le cas d'interventions obligatoires visant à tester ou à protéger un système d'information, par exemple lorsqu'une personne est chargée par une entreprise ou un vendeur de tester la résistance de son système de sécurité. Dans le cadre de la présente directive, les obligations contractuelles ou les conventions visant à limiter l'accès à des systèmes d'information par des conditions d'utilisation ou des conditions générales, ainsi que les conflits du travail concernant l'accès aux systèmes d'information d'un employeur et leur utilisation à des fins privées ne devraient pas engager de responsabilité pénale lorsque l'accès effectué dans ces conditions serait réputé non autorisé et constituerait donc la seule motivation des poursuites pénales. La présente directive est sans préjudice du droit d'accès à l'information tel que déterminé par le droit national et le droit de l'Union, et ne peut pas non plus servir pour justifier un accès illicite ou arbitraire à l'information.

(18) Les cyberattaques seraient susceptibles d'être facilitées par diverses circonstances, comme lorsque l'auteur a accès, dans le cadre de son activité professionnelle, aux systèmes de sécurité internes des systèmes d'information affectés. Dans le cadre du droit national, de telles circonstances devraient être prises en considération au cours des poursuites pénales le cas échéant.

(19) Les États membres devraient prévoir des circonstances aggravantes dans leur droit national conformément aux règles applicables établies en la matière par leur système juridique. Ils devraient veiller à ce que les juges puissent tenir compte de ces circonstances aggravantes lorsqu'ils prononcent une condamnation à l'encontre des auteurs d'infractions. Il relève de l'appréciation du juge d'évaluer ces circonstances avec les autres faits du cas considéré.

(20) La présente directive ne régit pas les conditions devant être remplies afin d'exercer une compétence à l'égard d'une des infractions qui y sont visées, telles qu'une déclaration de la victime sur le lieu de l'infraction, une dénonciation émanant de l'État du lieu où l'infraction a été commise, ou le fait que l'auteur de l'infraction n'ait pas fait l'objet de poursuites là où l'infraction a été commise.

(21) Dans le cadre de la présente directive, les États et les entités publiques restent pleinement tenus de garantir le respect des droits de l'homme et des libertés fondamentales, conformément aux obligations internationales existantes.

(22) La présente directive renforce l'importance des réseaux, tels que le réseau de points de contact du G8 ou celui du Conseil de l'Europe, disponibles vingt-quatre heures sur vingt-quatre et sept jours sur sept. ***Ces points de contact devraient donc pouvoir fournir une assistance effective, par exemple, faciliter l'échange d'informations disponibles pertinentes et la fourniture de conseils techniques ou d'informations juridiques*** aux fins des enquêtes ou des procédures portant sur des infractions pénales concernant des systèmes d'information et ***des données connexes impliquant l'État membre demandeur. Afin de garantir le bon fonctionnement des réseaux, chaque point de contact devrait être en mesure d'entrer rapidement en communication avec le point de contact d'un autre État membre, selon une procédure accélérée en s'appuyant entre autres sur un personnel formé et équipé***. Compte tenu de la rapidité avec laquelle des ***cyberattaques*** à grande échelle peuvent être menées, il conviendrait que les États membres soient en mesure de répondre promptement aux demandes urgentes émanant de ce réseau de points de contact. ***Dans pareils cas, il serait souhaitable que la demande d'informations s'accompagne d'un contact téléphonique afin de s'assurer que la demande est traitée rapidement par l'État membre auquel elle est adressée et qu'une réponse est apportée dans un délai de huit heures.***

(23) La coopération entre les pouvoirs publics d'un côté, et le secteur privé et la société civile, de l'autre, est essentielle pour prévenir les attaques contre les systèmes d'information et lutter contre celles-ci. Il est nécessaire de favoriser et d'améliorer la coopération entre les prestataires de services, les producteurs, les organismes chargés de l'application de la loi et les autorités judiciaires, tout en respectant pleinement l'état de droit. Cette coopération pourrait comprendre l'appui des prestataires de services pour aider à préserver des preuves éventuelles, fournir des éléments permettant d'identifier les auteurs d'infractions et, en dernier recours, fermer, totalement ou en partie, conformément au droit national et à la pratique nationale, les systèmes d'information ou les fonctions qui ont été compromis ou utilisés à des fins illégales. Les États membres devraient également envisager de mettre en place des réseaux de coopération et de partenariat avec les prestataires de service et les producteurs pour permettre l'échange d'informations relatives aux infractions relevant du champ d'application de la présente directive.

(24) Il est nécessaire de recueillir des données ***comparables*** sur les infractions prévues dans la présente directive. ***Des données pertinentes devraient être mises à la disposition des agences et organes spécialisés compétents de l'Union, comme Europol et ENISA, en fonction de leurs missions et de leurs besoins en information,*** afin d'avoir une vision plus complète du problème ***de la cybercriminalité et du niveau de sécurité des réseaux et de l'information au niveau de l'Union et de permettre ainsi de formuler une réponse plus efficace. Les États membres devraient transmettre à Europol et à son Centre européen de lutte contre la cybercriminalité des informations sur le mode opératoire des auteurs d'infractions, afin que ces agences puissent établir des évaluations de la menace et des analyses stratégiques en matière de cybercriminalité conformément à la décision 2009/371/JAI du Conseil du 6 avril 2009 portant création de l'Office européen de police (Europol)[1]. La communication d'informations peut aider à mieux comprendre les menaces actuelles et futures et contribuer ainsi à ce que des décisions plus appropriées et mieux ciblées soient prises pour combattre et prévenir les attaques contre les systèmes d'information.***

(25) La Commission devrait présenter un rapport sur l'application de la présente directive et faire les propositions législatives nécessaires, susceptibles de mener à un élargissement de son champ d'application, en prenant en compte les évolutions dans le domaine de la cybercriminalité. Au nombre de ces évolutions pourraient figurer les progrès technologiques, par exemple ceux permettant une exécution des lois plus efficace dans le domaine des attaques contre les systèmes d'information ou facilitant la prévention ou limitant l'impact de telles attaques. À cette fin, la Commission devrait prendre en considération les analyses et les rapports disponibles établis par les acteurs compétents, en particulier Europol et ENISA.

---

[1] ***JO L 121 du 15.5.2009, p. 37.***

(26) Afin de lutter efficacement contre la cybercriminalité, il est nécessaire de renforcer la résistance des systèmes d'information en prenant des mesures appropriées pour les protéger de manière plus efficace contre les cyberattaques. Les États membres devraient prendre les mesures nécessaires pour protéger leurs infrastructures critiques contre les cyberattaques, et examiner à cette occasion la protection de leurs systèmes d'information et des données qu'ils contiennent. Le fait que les personnes morales assurent un niveau adéquat de protection et de sécurité des systèmes d'information, par exemple lors de la fourniture de services de communications électroniques accessibles au public, conformément à la législation de l'Union en vigueur en matière de vie privée et de protection des communications électroniques et des données, est un élément essentiel d'une approche globale visant à lutter efficacement contre la cybercriminalité. Il convient de garantir des niveaux de protection appropriés contre les menaces et les vulnérabilités pouvant être raisonnablement identifiées en l'état des connaissances dans certains secteurs et compte tenu des situations spécifiques de traitement des données. Les coûts et charges liés à cette protection devraient être proportionnels au préjudice éventuel qu'une cyberattaque pourrait causer à ceux concernés. Les États membres sont encouragés à prévoir, dans le cadre de leur droit national, des mesures pertinentes permettant d'engager la responsabilité des personnes morales, lorsque celles-ci n'ont de toute évidence pas assuré un niveau de protection suffisant contre les cyberattaques.

(27) L'existence de lacunes et de différences importantes dans les législations ***et les procédures pénales*** des États membres en matière d'attaques contre les systèmes d'information ▌ risque d'entraver la lutte contre la criminalité organisée et le terrorisme, et de compliquer la coopération policière et judiciaire dans ce domaine. Les systèmes d'information modernes ayant un caractère transnational et ne connaissant pas de frontières, les attaques lancées contre eux ont une dimension ***transfrontière*** qui met en lumière la nécessité de prendre d'urgence des mesures complémentaires pour rapprocher le droit pénal dans ce domaine. Par ailleurs, il convient de faciliter la coordination des poursuites judiciaires dans les affaires relatives à des attaques contre des systèmes d'information par ***la mise en œuvre et l'application appropriées*** de la décision-cadre 2009/948/JAI du Conseil du 30 novembre 2009 relative à la prévention et au règlement des conflits en matière d'exercice de la compétence dans le cadre des procédures pénales[1]. ***Les États membres, en coopération avec l'Union, devraient également chercher à améliorer la coopération internationale en matière de sécurité des systèmes d'information, des réseaux informatiques et des données informatiques. Il convient de prendre dûment en considération la sécurité du transfert et du stockage des données dans tout accord international impliquant l'échange de données.***

[1] ***JO L 328 du 15.12.2009, p. 42.***

(28) Il est essentiel d'améliorer la coopération entre les services compétents chargés de l'application de la loi et les autorités judiciaires à travers l'Union pour pouvoir lutter efficacement contre la cybercriminalité. Dans ce contexte, il convient d'encourager l'intensification des efforts visant à offrir une formation adaptée aux autorités compétentes de manière à ce qu'elles comprennent mieux la cybercriminalité et son impact et à favoriser la coopération et l'échange de bonnes pratiques, par exemple via les agences et organes spécialisés compétents de l'Union. Cette formation devrait notamment viser à mieux faire connaître les différents systèmes juridiques nationaux, les éventuels défis juridiques et techniques qui se présentent dans les enquêtes pénales et la répartition des compétences entre les autorités nationales compétentes.

▌

(29) La présente directive respecte les droits de l'homme ***et*** les ***libertés*** fondamentales et est conforme aux principes consacrés en particulier par la charte des droits fondamentaux de l'Union européenne ***et la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales***, notamment la protection des données à caractère personnel, ***le droit au respect de la vie privée***, la liberté d'expression et d'information, le droit à un procès équitable, la présomption d'innocence et les droits de la défense, ainsi que les principes de légalité et de proportionnalité des infractions et sanctions pénales. La présente directive tend en particulier à garantir le plein respect de ces droits et principes et doit être mise en œuvre en conséquence.

(30) La protection des données à caractère personnel est un droit fondamental en vertu de l'article 16, paragraphe 1, du traité sur le fonctionnement de l'Union européenne, et de l'article 8 de la charte des droits fondamentaux de l'Union européenne. Par conséquent, tout traitement de données à caractère personnel effectué dans le cadre de la mise en œuvre de la présente directive devrait être conforme au droit de l'Union en matière de protection des données.

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

(32) 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, le Danemark ne participe pas à l'adoption de la présente directive et n'est pas lié par celle-ci ni soumis à son application.

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

(34) La présente directive vise à modifier et à étendre les dispositions de la décision-cadre 2005/222/JAI du Conseil du 24 février 2005 relative aux attaques visant les systèmes d'information[1]. Puisque les modifications à faire sont significatives par leur nombre comme par leur nature, il convient, pour plus de clarté, de remplacer entièrement la décision-cadre 2005/222/JAI à l'égard des États membres qui participent à l'adoption de la présente directive,

ONT ADOPTÉ LA PRÉSENTE DIRECTIVE:

---

1 ***JO L 69 du 16.3.2005, p. 67.***

Article premier

Objet

La présente directive fixe des règles minimales concernant la définition des infractions pénales et les sanctions en matière d'attaques contre les systèmes d'information. Elle vise également à faciliter la prévention de ces infractions et à améliorer la coopération entre les autorités judiciaires et les autres autorités compétentes.

Article 2

Définitions

Aux fins de la présente directive, on entend par:

a) "système d'information": un dispositif isolé ou un ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données informatiques, ainsi que les données informatiques stockées, traitées, récupérées ou transmises par ce dispositif ou cet ensemble de dispositifs en vue du fonctionnement, de l'utilisation, de la protection et de la maintenance de celui-ci;

b) "données informatiques": une représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système d'information exécute une fonction;

c) "personne morale": une entité à laquelle le droit en vigueur reconnaît le statut de personne morale, à l'exception des États ou des entités publiques agissant dans l'exercice de prérogatives de puissance publique, ou des organisations internationales relevant du droit public;

d) "sans droit": ***un comportement*** visé dans la présente directive, y compris un accès, une atteinte à l'intégrité ou une interception, qui n'est pas autorisé par le propriétaire du système ou d'une partie du système ou un autre titulaire de droits sur celui-ci ou une partie de celui-ci, ou n'est pas permis par le droit national.

Article 3

Accès illégal à des systèmes d'information

Les États membres prennent les mesures nécessaires pour ériger en infraction pénale punissable l'accès sans droit, ***lorsqu'il est intentionnel***, à tout ou partie d'un système d'information, ***lorsque l'acte est commis en violation d'une mesure de sécurité***, au moins lorsqu'il ne s'agit pas de cas mineurs.

Article 4

Atteinte illégale à l'intégrité d'un système

Les États membres prennent les mesures nécessaires pour ériger en infraction pénale punissable ▌ le fait de provoquer une perturbation grave ou une interruption du fonctionnement d'un système d'information, en introduisant, transmettant, endommageant, effaçant, détériorant, altérant, supprimant ou rendant inaccessibles des données informatiques lorsque l'acte est commis ***de manière intentionnelle*** et sans droit, au moins lorsqu'il ne s'agit pas de cas mineurs.

Article 5

Atteinte illégale à l'intégrité des données

Les États membres prennent les mesures nécessaires pour ériger en infraction pénale punissable ▌ le fait d'effacer, d'endommager, de détériorer, d'altérer, de supprimer ou de rendre inaccessibles des données informatiques d'un système d'information lorsque l'acte est commis ***de manière intentionnelle*** et sans droit, au moins lorsqu'il ne s'agit pas de cas mineurs.

Article 6

Interception illégale

Les États membres prennent les mesures nécessaires pour ériger en infraction pénale punissable ▌ l'interception, effectuée par des moyens techniques, de transmissions non publiques de données informatiques à destination, en provenance ou à l'intérieur d'un système d'information, y compris les émissions électromagnétiques provenant d'un système d'information transportant de telles données informatiques, lorsque l'acte est commis ***de manière intentionnelle et sans droit, au moins*** lorsqu'il ne s'agit pas de cas mineurs.

Article 7

Outils utilisés pour commettre les infractions

Les États membres prennent les ***mesures*** nécessaires pour ériger en infraction pénale punissable la production, la vente, l'obtention pour utilisation, l'importation, ▌ la diffusion ou d'autres formes de mise à disposition intentionnelles d'un des outils suivants lorsque l'acte est commis sans droit et ***dans l'intention de l'utiliser*** pour commettre l'une des infractions visées aux articles 3 à 6, ***au moins*** lorsqu'il ne s'agit pas de cas mineurs***:***

a) ▌ un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions visées aux articles 3 à 6;

b) un mot de passe, un code d'accès ou des données informatiques similaires permettant d'accéder à tout ou partie d'un système d'information.

Article 8

***Incitation, participation et** complicité, **et** tentative*

1. Les États membres veillent 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.

2. Les États membres veillent à ériger en infraction pénale punissable la tentative de commettre ***une infraction*** visée aux ***articles 4 et 5***.

Article 9

Sanctions

1. Les États membres prennent les mesures nécessaires pour faire en sorte que les infractions visées aux articles 3 à 8 soient passibles de sanctions pénales effectives, ***proportionnées*** et dissuasives.

2. Les États membres prennent les mesures nécessaires pour faire en sorte que les infractions visées aux articles 3 à 7 soient passibles ***d'une peine d'emprisonnement maximale d'au moins deux ans***, ***au moins*** lorsqu'il ne s'agit pas de cas mineurs**.**

3. Les États membres prennent les mesures nécessaires pour faire en sorte que les infractions visées aux articles 4 et 5 soient passibles d'une peine d'emprisonnement maximale d'au moins trois ans lorsqu'elles sont commises de manière intentionnelle et qu'un nombre important de systèmes d'information est atteint au moyen d'un des outils visés à l'article 7.

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

a) elles sont commises dans le cadre d'une organisation criminelle telle que définie dans la décision-cadre 2008/841/JAI, indépendamment de la sanction qui y est prévue, ou

b) elles causent un préjudice grave, ou

c) elles sont commises contre un système d'information d'une infrastructure critique.

5. ***Les États membres prennent les mesures nécessaires pour 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, conformément au droit national, 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.***

▌

Article 10

Responsabilité des personnes morales

1. Les États membres prennent les mesures nécessaires pour que les personnes morales puissent être tenues pour responsables des infractions visées aux articles 3 à 8, lorsqu'elles sont commises pour leur compte par toute personne agissant soit individuellement soit en tant que membre d'un organe de la personne morale en cause, et qui exerce un pouvoir de direction en son sein fondé sur:

a) un pouvoir de représentation de la personne morale;

b) une autorité pour prendre des décisions au nom de la personne morale;

c) une autorité pour exercer un contrôle au sein de la personne morale.

2. Les États membres prennent les mesures nécessaires pour s'assurer que les personnes morales puissent être tenues pour responsables lorsque l'absence de surveillance ou de contrôle de la part d'une personne visée au paragraphe 1 a rendu possible la commission de l'une des infractions visées aux articles 3 à 8 pour le compte de ladite personne morale, par une personne soumise à son autorité.

3. La responsabilité des personnes morales au titre des paragraphes 1 et 2 n'exclut pas les poursuites pénales contre les personnes physiques auteurs, ***instigatrices*** ou complices de l'une des infractions visées aux articles 3 à 8.

Article 11

Sanctions à l'encontre des personnes morales

1. Les États membres prennent les mesures nécessaires pour qu'une personne morale déclarée responsable au titre de l'article 10, paragraphe 1, soit passible de sanctions effectives, proportionnées et dissuasives, qui incluent des amendes pénales ou non pénales, et éventuellement d'autres sanctions, telles que:

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

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

c) le placement sous surveillance judiciaire;

d) une mesure judiciaire de dissolution;

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

2. Les États membres prennent les mesures nécessaires pour qu'une personne morale déclarée responsable au titre de l'article 10, paragraphe 2, soit passible de sanctions ou d'autres mesures effectives, proportionnées et dissuasives.

Article 12

Compétence

1. Les États membres établissent leur compétence à l'égard des infractions visées aux articles 3 à 8, lorsque l'infraction a été commise:

a) en tout ou en partie sur leur territoire; ou

b) ***par un de leurs ressortissants, au moins dans les cas où l'acte constitue une infraction là où il a été commis.***

▌

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

a) l'auteur de l'infraction a commis celle-ci alors qu'il était physiquement présent sur son territoire, que l'infraction vise un système d'information situé sur son territoire ou non; ou

b) l'infraction vise un système d'information situé sur son territoire, que l'auteur de l'infraction soit physiquement présent sur son territoire ou non lors de la commission de l'infraction.

3. Un État membre informe la Commission de sa décision d'établir sa compétence à l'égard des infractions visées aux articles 3 à 8 qui ont été commises en dehors de son territoire, notamment dans les cas suivants:

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

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

Article 13

Échange d'informations

1. Aux fins de l'échange d'informations relatives aux infractions visées aux articles 3 à 8, ***les États membres veillent à disposer d'un point de contact national opérationnel*** et à recourir au réseau existant de points de contact opérationnels, disponibles vingt-quatre heures sur vingt-quatre et sept jours sur sept. Les États membres veillent également à mettre en place des procédures afin que, ***en cas de demandes urgentes d'assistance, l'autorité compétente indique, dans un délai de huit heures à compter de la réception de la demande, au moins si la demande sera satisfaite, et la forme et le délai estimé pour cette réponse.***

2. Les États membres communiquent à la Commission le point de contact visé au paragraphe 1 qu'ils ont désigné. La Commission transmet ces informations aux autres États membres et ***aux agences et organes spécialisés compétents de l'Union.***

3. Les États membres prennent les mesures nécessaires pour faire en sorte que des canaux de communication appropriés soient mis à disposition afin de faciliter la notification sans retard indu aux autorités nationales compétentes des infractions visées aux articles 3 à 6.

Article 14

Suivi et statistiques

1. Les États membres veillent à mettre en place un système d'enregistrement, de production et de communication de statistiques sur les infractions visées aux articles 3 ***à 7.***

2. Les statistiques visées au paragraphe 1 portent, au minimum, sur les ***données existantes*** concernant le nombre d'infractions visées aux articles 3 à 7 ***enregistrées par*** les États membres, ainsi que ▌ le nombre de personnes ***poursuivies et condamnées*** pour les infractions visées aux articles 3 ***à 7.***

3. Les États membres transmettent à la Commission les données recueillies en vertu du présent article. La ***Commission veille*** à ce qu'un état consolidé des rapports statistiques soit publié et ***soumis aux agences et organes spécialisés compétents de l'Union.***

Article 15

Remplacement *de la décision-cadre 2005/222/JAI*

La décision-cadre 2005/222/JAI ***est remplacée à l'égard des États membres qui participent à l'adoption de la présente directive***, sans préjudice des obligations des États membres concernant ***le délai*** de transposition ***de la décision-cadre*** en droit national.

À l'égard des États membres participant à l'adoption de la présente directive, ***les références faites*** à la décision-cadre ***2005/222/JAI*** s'entendent comme faites à la présente directive.

Article 16

Transposition

1. Les États membres mettent en vigueur les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive au plus tard le ...[*] .

[*] ***JO: prière d'insérer la date correspondant à deux ans après la date d'entrée en vigueur de la présente directive.***

2. Les États membres communiquent à la Commission le texte des dispositions transposant dans leur droit national les obligations que leur impose la présente directive.

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

Article 17

Rapports

La Commission présente au Parlement européen et au Conseil, au plus tard le ...*, un rapport évaluant dans quelle mesure les États membres ont pris les dispositions nécessaires pour se conformer à la présente directive, accompagné, le cas échéant, de propositions législatives. La Commission tient également compte des évolutions techniques et juridiques dans le domaine de la cybercriminalité, en particulier au regard du champ d'application de la présente directive.

▌

* ***JO: prière d'insérer la date correspondant à quatre ans après la date d'entrée en vigueur de la présente directive.***

Article 18

Entrée en vigueur

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

Article 19

Destinataires

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

Fait à ...,

Par le Parlement européen
Le Président

Par le Conseil
Le Président