E 5692

ASSEMBLÉE NATIONALE

TREIZIÈME LÉGISLATURE

SÉNAT

SESSION ORDINAIRE DE 2010-2011

Reçu à la Présidence de l'Assemblée nationale
le 8 octobre 2010

Enregistré à la Présidence du Sénat
le 8 octobre 2010

TEXTE SOUMIS EN APPLICATION DE L'ARTICLE 88-4 DE LA CONSTITUTION

PAR LE GOUVERNEMENT,

À L'ASSEMBLÉE NATIONALE ET AU SÉNAT.

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) 517 final

CONSEIL DE L'UNION EUROPÉENNE

Bruxelles, le 4 octobre 2010 (05.10)
(OR. en)

14436/10

Dossier interinstitutionnel: 2010/0273 (COD)

DROIPEN 107
TELECOM 100
CODEC 952

PROPOSITION

Origine:	Commission européenne
En date du:	30 septembre 2010
Objet:	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

Les délégations trouveront ci-joint la proposition de la Commission transmise par lettre de Monsieur Jordi AYET PUIGARNAU, Directeur, à Monsieur Pierre de BOISSIEU, Secrétaire général du Conseil de l'Union européenne.

p.j.: COM(2010) 517 final

COMMISSION EUROPÉENNE

Bruxelles, le 30.9.2010
COM(2010) 517 final

2010/0273 (COD)

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

{SEC(2010) 1122 final}
{SEC(2010) 1123 final}

EXPOSÉ DES MOTIFS

1. MOTIVATION ET OBJECTIFS DE LA PROPOSITION

La présente proposition a pour objet de remplacer la décision-cadre 2005/222/JAI du Conseil du 24 février 2005 relative aux attaques visant les systèmes d'information[1]. Ainsi qu'il ressort de ses considérants, la décision-cadre visait à renforcer la coopération entre les autorités judiciaires et les autres autorités compétentes, notamment la police et les autres services spécialisés chargés de l'application de la loi dans les États membres, grâce à un rapprochement de leurs règles pénales réprimant les attaques contre les systèmes d'information. Elle créait ainsi une législation européenne permettant de poursuivre des infractions telles que l'accès illicite à un système d'information, l'atteinte à l'intégrité d'un système et l'atteinte à l'intégrité des données, ainsi que des dispositions spécifiques relatives à la responsabilité des personnes morales, la compétence juridictionnelle et les échanges d'informations. Les États membres étaient tenus de prendre les mesures nécessaires à sa transposition le 16 mars 2007 au plus tard.

Le 14 juillet 2008, la Commission a publié un rapport sur la transposition de la décision-cadre[2]. Le rapport concluait que des progrès notables avaient été enregistrés dans la plupart des États membres et que le degré de mise en œuvre était relativement bon, mais que certains États membres n'avaient pas encore achevé la transposition. Il mentionnait ensuite que «les récentes attaques perpétrées en Europe depuis l'adoption de la décision-cadre ont souligné l'émergence de [plusieurs] menaces, que constituent notamment les attaques massives commises simultanément contre plusieurs systèmes d'information et l'utilisation accrue des "botnets" à des fins criminelles.» Ce type d'attaques n'était pas au centre des attentions lors de l'adoption de la décision-cadre. Pour faire face à ces évolutions, la Commission envisagerait l'adoption de mesures afin de trouver de meilleures solutions pour répondre à cette menace (voir les paragraphes suivants pour l'explication des «botnets»).

L'importance de nouvelles actions en vue d'intensifier la lutte contre la cybercriminalité avait été soulignée dans le programme de La Haye de 2004 visant à renforcer la liberté, la sécurité et la justice dans l'Union européenne, ainsi dans le programme de Stockholm de 2009 et son plan d'action[3]. En outre, la récente stratégie numérique pour l'Europe[4], première initiative phare adoptée dans le cadre de la stratégie Europe 2020, a constaté la nécessité de réagir au développement de nouvelles formes de criminalité, notamment la cybercriminalité au niveau européen. Dans ce domaine d'action où la confiance et la sécurité sont primordiales, la Commission est déterminée à adopter des mesures pour lutter contre les attaques visant les systèmes d'information.

Au plan international, la convention du Conseil de l'Europe sur la cybercriminalité («convention sur la cybercriminalité»), signée le 23 novembre 2001, est considérée comme la norme internationale la plus aboutie à l'heure actuelle, car elle crée un cadre exhaustif et cohérent couvrant la diversité des aspects de la cybercriminalité[5]. À ce jour, si la convention a

---

1 JO L 69 du 16.3.2005, p. 68.

2 Rapport de la Commission au Conseil fondé sur l'article 12 de la décision-cadre du Conseil du 24 février 2005 relative aux attaques visant les systèmes d'information - COM(2008) 448.

3 JO C 198 du 12.8.2005, JO C 115 du 4.5.2010, COM(2010) 171 du 20.4.2010.

4 Communication de la Commission - COM (2010) 245 du 19.5.2010.

5 Convention du Conseil de l'Europe sur la cybercriminalité, Budapest 23.11.2001, CETS n° 185.

été signée par les 27 États membres, elle n'a été ratifiée que par 15 d'entre eux[6]. Elle est entrée en vigueur le 1er juillet 2004. L'Union européenne ne figure pas parmi ses signataires. En raison de l'importance de cet instrument, la Commission encourage activement les autres États membres de l'UE à ratifier la convention dès que possible.

- **Contexte général**

La cause première de la cybercriminalité est la vulnérabilité, qui résulte de divers facteurs. L'insuffisance des mesures prises dans le cadre des mécanismes répressifs pour lutter contre ce phénomène contribue à sa prévalence et complique la situation, certains types d'infractions ayant un caractère transnational. Le signalement de ces infractions est souvent insuffisant, d'une part parce que certaines passent inaperçues, d'autre part parce que les victimes (opérateurs économiques et entreprises) ne les dénoncent pas, de peur que l'exposition publique de leurs vulnérabilités n'atteigne leur réputation et ne compromette leurs perspectives commerciales.

En outre, les divergences entre législations et procédures pénales nationales peuvent donner lieu à des différences dans les enquêtes et les poursuites pénales, si bien que le traitement réservé à ces infractions ne sera pas uniforme. L'évolution des technologies de l'information aggrave encore le problème en facilitant la production et la distribution des outils («maliciels» et «botnets»), tout en offrant l'anonymat aux délinquants et en éparpillant la responsabilité entre divers pays. La difficulté d'engager des poursuites qui en résulte permet ainsi à la criminalité organisée de réaliser des profits considérables à peu de risques.

La présente proposition tient compte des nouvelles méthodes adoptées pour commettre des infractions informatiques, notamment le recours aux «botnets» ou «réseaux zombies». Ce terme désigne un groupe d'ordinateurs qui ont été contaminés par des logiciels malveillants (virus informatiques). Un tel réseau d'ordinateurs compromis («zombies») peut être activé pour exécuter certaines actions, comme attaquer des systèmes d'information (cyberattaques). Les «zombies» peuvent être contrôlés, souvent à l'insu des utilisateurs de ces ordinateurs, par un autre ordinateur, également appelé «centre de commande et de contrôle». Les personnes qui gèrent ce centre font partie des auteurs de l'infraction puisqu'elles utilisent les ordinateurs compromis pour attaquer des systèmes d'information. Il est très difficile de repérer les coupables car les ordinateurs qui composent le réseau zombie et lancent l'attaque peuvent se trouver ailleurs.

Les attaques par réseaux zombies sont souvent réalisées à grande échelle, c'est-à-dire avec des outils qui atteignent un grand nombre de systèmes d'information (ordinateurs) ou en causant un préjudice considérable, eu égard aux services de réseau perturbés, au coût financier, aux pertes de données à caractère personnel, etc. Par conséquent, un «grand réseau zombie» aurait la capacité de causer un grave préjudice. Il n'est pas aisé de définir la taille des réseaux zombies mais les plus grands qui ont été observés auraient, d'après les estimations, entre 40 000 et 100 000 connexions (c'est-à-dire ordinateurs contaminés) par période de 24 heures[7].

---

6 Pour l'état des ratifications de la convention (CETS n° 185), voir: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=FRE

7 Le nombre de connexions par 24 heures est l'unité de mesure couramment utilisée pour estimer la taille des réseaux zombies.

- **Dispositions en vigueur dans le domaine de la proposition**

Au niveau de l'Union, la décision-cadre introduit un niveau minimal de rapprochement des législations des États membres pour incriminer plusieurs infractions informatiques, notamment l'accès illicite à un système d'information, l'atteinte à l'intégrité d'un système, l'atteinte à l'intégrité des données, ainsi que l'instigation, la complicité et la tentative d'infraction.

Bien que les dispositions de la décision-cadre aient été transposées par les États membres dans l'ensemble, le texte comporte plusieurs failles, imputables à l'évolution de la taille et du nombre d'infractions (cyberattaques). En effet, il ne rapproche les législations que sur un nombre limité d'infractions et ne permet pas de faire face à la menace potentielle que les attaques à grande échelle représentent pour la société. Il ne tient pas non plus suffisamment compte de la gravité des infractions et ne prévoit pas de sanctions à leur mesure.

D'autres initiatives et programmes de l'Union, existants ou en préparation, tentent de résoudre les difficultés liées aux cyberattaques ou aux problèmes informatiques, tels que la sécurité des réseaux ou des utilisateurs de l'internet. Il s'agit notamment des actions financées par les programmes «Prévenir et combattre la criminalité»[8], «Justice pénale»[9], «Pour un internet plus sûr»[10] et par l'initiative relative aux infrastructures d'information critiques[11]. Outre la décision-cadre, un autre instrument juridique pertinent est la décision-cadre 2004/68/JAI relative à la lutte contre l'exploitation sexuelle des enfants et la pédopornographie.

Au plan administratif, la pratique consistant à contaminer des ordinateurs pour les transformer en «zombies» est déjà prohibée par les règles européennes de protection des données et de la vie privée[12]. Des services administratifs nationaux ont ainsi commencé à coopérer au sein du Réseau de contact européen des autorités anti-pourriel. Ces règles font obligation aux États membres d'interdire l'interception des communications sur les réseaux publics de communications et les services de communication électronique accessibles au public sans le consentement des utilisateurs concernés ou l'autorisation de la loi.

La présente proposition est conforme à ces règles. Les États membres devraient s'attacher à améliorer la coopération entre les autorités administratives et répressives pour les cas passibles de sanctions à la fois administratives et pénales.

- **Cohérence avec les autres politiques et objectifs de l'Union**

Les objectifs sont compatibles avec les politiques de l'Union destinées à combattre la criminalité organisée, augmenter la résilience des réseaux informatiques, protéger les infrastructures d'information critiques, et la protection des données. Ils sont également compatibles avec le programme «Pour un internet plus sûr» créé pour promouvoir une utilisation plus sûre de l'internet et des nouvelles technologies en ligne, et pour lutter contre les contenus illicites.

---

8 Voir: http://ec.europa.eu/justice_home/funding/isec/funding_isec_en.htm

9 Voir: http://ec.europa.eu/justice_home/funding/jpen/funding_jpen_en.htm

10 Voir: http://ec.europa.eu/information_society/activities/sip/index_en.htm

11 Voir: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

12 Directive vie privée et communications électroniques (JO L 201 du 31.7.2002), modifiée par la directive 2009/136/CE (JO L 337 du 18.12.2009).

La proposition a fait l'objet d'un examen approfondi pour vérifier que ses dispositions sont totalement compatibles avec les droits fondamentaux et, notamment, la protection des données à caractère personnel, la liberté d'expression et d'information, le droit à un procès équitable, la présomption d'innocence et le droit à la défense, ainsi qu'avec les principes de légalité et de proportionnalité des infractions et sanctions pénales.

2. CONSULTATION DES PARTIES INTÉRESSÉES ET ANALYSE D'IMPACT

- **Consultation des parties intéressées**

Un large éventail d'experts du domaine a été consulté dans le cadre de plusieurs réunions différentes abordant les divers aspects de la lutte contre la cybercriminalité, y compris les suites judiciaires (action pénale) de ces infractions. Il s'agissait, entre autres, de représentants des autorités publiques et du secteur privé des États membres, de magistrats spécialisés, d'organisations internationales, d'agences européennes et d'organismes spécialisés. Plusieurs experts et organisations ont ultérieurement envoyé des articles et fourni des informations.

Les principales conclusions tirées de la consultation sont les suivantes:

– nécessité d'une intervention de l'Union dans ce domaine;

– nécessité d'incriminer les formes d'infraction qui ne figurent pas dans la décision-cadre, en particulier les nouvelles formes de cyberattaques («réseaux zombies»);

– nécessité de lever les obstacles aux enquêtes et poursuites dans les affaires transfrontières.

Les informations recueillies au cours de la consultation ont été prises en considération dans l'analyse d'impact.

Obtention et utilisation d'expertise

L'expertise externe a été obtenue pendant les diverses réunions avec les parties concernées.

Analyse d'impact

Diverses options d'action ont été étudiées pour atteindre l'objectif.

- Option (1): Statu Quo / Pas de nouvelle action de l'Union

Cette option implique que l'Union ne prenne aucune initiative supplémentaire pour lutter contre le type particulier d'infraction informatique que constituent les attaques visant les systèmes d'information. Les actions en cours se poursuivront, notamment les programmes destinés à renforcer la protection des infrastructures d'information critiques et à améliorer la coopération public-privé dans la lutte contre la cybercriminalité.

- Option (2): Élaboration d'un programme intensifiant les efforts de lutte contre les attaques visant les systèmes d'information par des mesures non législatives

Parallèlement au programme de protection des infrastructures d'information critiques, des mesures non législatives seraient axées sur la répression transfrontières et la coopération public-privé. Ces instruments non contraignants devraient encourager une action plus

coordonnée au niveau de l'Union, notamment la consolidation de l'actuel réseau 24/7 de points de contact des forces de l'ordre; la mise en place d'un réseau européen de points de contact public-privé réunissant les experts en cybercriminalité et les forces de l'ordre; l'élaboration d'un modèle européen d'accord sur le niveau de service pour la coopération des services répressifs avec des opérateurs du secteur privé; et le soutien à l'organisation de programmes de formation aux enquêtes sur la cybercriminalité, destinés aux forces de l'ordre.

- Option (3): Mise à jour sélective des dispositions de la décision-cadre (nouvelle directive remplaçant cette dernière) pour répondre à la menace d'attaques à grande échelle contre des systèmes d'information (réseaux zombies) et, lorsqu'elles sont commises en dissimulant l'identité réelle de l'auteur et en causant un préjudice au titulaire légitime de l'identité, pour accroître l'efficacité des points de contact des services répressifs des États membres et combler le manque de statistiques sur les cyberattaques.

Cette option prévoit l'introduction d'une législation spécifique ciblée (c'est-à-dire limitée) pour prévenir les attaques à grande échelle contre des systèmes d'information. Cette législation renforcée s'accompagnerait de mesures non législatives en vue d'intensifier la coopération opérationnelle transfrontières contre ces attaques, ce qui faciliterait l'application des mesures législatives. Toutes ces dispositions serviraient à améliorer la préparation, la sécurité et la résilience des infrastructures d'information critiques et à échanger les bonnes pratiques.

- Option (4): Adoption d'un corpus complet de législation européenne contre la cybercriminalité

Cette option impliquerait une nouvelle législation européenne complète. Outre l'adoption des mesures non contraignantes prévues dans l'option 2 et la mise à jour mentionnée dans l'option 3, cette solution aborderait également d'autres problèmes juridiques liés à l'utilisation de l'internet. En effet, les mesures ne concerneraient pas seulement les attaques contre les systèmes d'information mais également des problèmes tels que la cyberdélinquance financière, les contenus illégaux sur l'internet, les collectes/stockages/transferts de preuves électroniques, et elles détailleraient davantage les règles de compétence. La législation serait applicable parallèlement à la convention du Conseil de l'Europe sur la cybercriminalité et intégrerait les mesures non législatives d'accompagnement précitées.

- Option (5): Mise à jour de la convention du Conseil de l'Europe sur la cybercriminalité

Cette option obligerait à renégocier une bonne partie de la convention actuelle, ce qui prendrait du temps et ne serait donc pas compatible avec le calendrier d'action proposé dans l'analyse d'impact. Il ne semble d'ailleurs pas y avoir de volonté internationale de renégocier la convention. La mise à jour de cette dernière ne saurait donc être considérée comme une option réalisable puisqu'elle dépasserait le délai d'action prescrit.

Option privilégiée: combinaison entre des mesures non législatives (option 2) et une mise à jour sélective de la décision-cadre (option 3)

Au terme d'une analyse des incidences économiques, sociales et sur les droits fondamentaux, les options 2 et 3 représentent la meilleure façon de résoudre le problème et d'atteindre les objectifs de la proposition.

Lors de l'élaboration de la présente proposition, la Commission a réalisé une analyse d'impact.

3. ÉLÉMENTS JURIDIQUES DE LA PROPOSITION

- **Résumé de l'action proposée**

Tout en abrogeant la décision-cadre 2005/222/JAI, la directive reprendra ses dispositions actuelles et inclura les nouveaux éléments décrits ci-après.

– S'agissant du droit pénal matériel en général, la directive:

A. incrimine la production, la vente, l'acquisition en vue de l'utilisation, l'importation, la distribution ou la mise à disposition par d'autres moyens de dispositifs/outils utilisés pour commettre les infractions;

B. prévoit des circonstances aggravantes:

- la grande ampleur des attaques – les réseaux zombies ou dispositifs similaires seraient incriminés en créant de nouvelles circonstances aggravantes, en ce sens que la mise en place d'un réseau zombie ou d'un dispositif similaire constituerait un facteur aggravant lors de la commission des infractions énumérées dans la décision-cadre existante;

- lorsque les attaques sont commises en dissimulant l'identité réelle de l'auteur et en causant un préjudice au titulaire légitime de l'identité. Toutes ces dispositions devraient être conformes aux principes de légalité et de proportionnalité des infractions et sanctions pénales, et être compatibles avec la législation existante sur la protection des données à caractère personnel[13];

C. crée l'infraction d'«interception illégale»;

D. introduit des mesures pour améliorer la coopération européenne en matière de justice pénale en consolidant la structure existante des points de contact 24/7[14]:

- l'obligation de donner suite à une demande d'assistance émise par les points de contact opérationnels (visés à l'article 14 de la directive) dans un certain délai est proposée. La convention sur la cybercriminalité ne comporte en effet aucune disposition obligatoire à ce sujet. Cette mesure a pour but d'assurer que les points de contact indiquent dans un délai déterminé s'ils sont en mesure de répondre à la demande d'assistance et dans quel délai le point de contact demandeur peut attendre la solution au problème soumis. Le contenu exact des solutions n'est pas précisé;

E. répond au besoin d'établir des statistiques sur les infractions informatiques en faisant obligation aux États membres de mettre en place un dispositif approprié d'enregistrement, de production et de communication de statistiques sur les

---

13 Comme la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37) (en cours de révision), et comme la directive générale sur la protection des données (directive 95/46/CE).

14 Créés par la convention et visés par la décision-cadre 2005/222/JAI relative aux attaques visant les systèmes d'information.

infractions énumérées dans la décision-cadre existante et la nouvelle infraction d'«interception illégale».

Dans les définitions des infractions pénales énumérées aux articles 3, 4, 5 (accès illégal à des systèmes d'information, atteinte à l'intégrité d'un système et atteinte à l'intégrité des données), la directive contient une disposition qui permet de n'incriminer que les «cas qui ne sont pas sans gravité» lors de la transposition de la directive en droit national. Cette flexibilité a pour but de permettre aux États membres de ne pas inclure les cas qui seraient in abstracto couverts par la définition de base, mais dont il est considéré qu'ils ne nuisent pas à l'intérêt juridique protégé, par exemple des actes commis par des jeunes gens qui veulent prouver leur savoir-faire en technologies de l'information. Cette possibilité de limiter la portée de l'incrimination ne devrait cependant pas conduire à l'introduction d'autres éléments constitutifs d'infraction que ceux déjà prévus par la directive, car il s'ensuivrait que seules les infractions commises dans des circonstances aggravantes seraient couvertes. Lors de la transposition, les États membres devraient notamment s'abstenir d'ajouter d'autres éléments constitutifs aux infractions de base, comme, par exemple, une intention particulière de tirer des revenus illicites d'une infraction ou l'existence d'une conséquence spécifique, comme un préjudice considérable.

- **Base juridique**

Article 83, paragraphe 1, du traité sur le fonctionnement de l'Union européenne[15].

- **Principe de subsidiarité**

Le principe de subsidiarité s'applique aux actions de l'Union européenne. Les objectifs de la proposition ne peuvent pas être réalisés de manière suffisante par les États membres pour les raisons suivantes:

la cybercriminalité et, plus particulièrement, les attaques visant les systèmes d'information ont une dimension transfrontières considérable qui se manifeste très nettement dans les attaques à grande échelle, puisque les éléments de connexion d'une attaque sont souvent installés dans des lieux et des pays différents. Une action au niveau de l'Union s'impose donc, notamment pour ne pas se laisser dépasser par la tendance actuelle consistant à lancer des attaques à grande échelle en Europe et dans le monde. Cette action au niveau de l'Union et la mise à jour de la décision-cadre 2005/222/JAI avaient d'ailleurs été évoquées dans les conclusions du Conseil de novembre 2008[16], car l'objectif de protéger efficacement les citoyens contre les infractions informatiques ne peut être atteint de manière suffisante par les seuls États membres.

Les objectifs de la proposition peuvent être mieux réalisés au niveau de l'Union pour les raisons suivantes:

la proposition poursuivra le rapprochement du droit pénal des États membres et de leurs règles de procédure, ce qui aura un effet positif sur la lutte contre ces infractions. Premièrement, c'est un moyen d'empêcher les délinquants d'aller s'installer dans des États membres ayant une législation plus laxiste à l'égard des attaques informatiques.

---

15 JO C 83 du 30.3.2010, p. 49.

16 "Une stratégie de travail concertée et des mesures concrètes de lutte contre la cybercriminalité", 2987e session du Conseil «Justice et Affaires intérieures», Bruxelles, 27-28 novembre 2008.

Deuxièmement, les définitions communes permettent d'échanger des informations et de rassembler et comparer les données pertinentes. Troisièmement, cela accroît l'efficacité des mesures de prévention dans toute l'Union et la coopération internationale.

La proposition est donc conforme au principe de subsidiarité.

- **Principe de proportionnalité**

La présente proposition est conforme au principe de proportionnalité pour la raison suivante:

la présente directive se limite au minimum requis pour atteindre ces objectifs au niveau européen et n'excède pas ce qui est nécessaire à cette fin, compte tenu de la nécessité de disposer d'une législation pénale précise.

- **Choix des instruments**

Instrument proposé: directive.

D'autres moyens ne seraient pas appropriés pour la raison suivante:

la base juridique impose une directive.

Des mesures non législatives et une autoréglementation amélioreraient certes la situation dans certains domaines où la mise en œuvre est capitale, mais auraient de piètres résultats dans d'autres domaines où il est essentiel d'adopter une nouvelle législation.

4. INCIDENCES BUDGÉTAIRES

La proposition a une faible incidence sur le budget de l'Union. Plus de 90% du coût, estimé à EUR 5 913 000, seraient supportés par les États membres et il est possible de demander un financement de l'Union pour réduire le coût.

5. INFORMATIONS SUPPLÉMENTAIRES

- **Abrogation de la législation existante**

L'adoption de la proposition entraînera l'abrogation de la législation existante.

- **Champ d'application territorial**

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

2010/0273 (COD)

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

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[17],

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

vu l'avis du Comité économique et social européen,

vu l'avis du Comité des régions,

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(1) La présente directive a pour objet de rapprocher les règles pénales appliquées par les États membres pour réprimer les attaques contre les systèmes d'information et de renforcer la coopération entre les autorités judiciaires et les autres autorités compétentes, notamment la police et les autres services spécialisés chargés de l'application de la loi dans les États membres.

(2) Les attaques contre les systèmes d'information, en particulier celles qui pourraient émaner du milieu de la criminalité organisée, constituent une menace croissance, et l'éventualité d'attaques terroristes ou politiques contre les systèmes d'information des infrastructures critiques des États membres et de l'Union suscite de plus en plus l'inquiétude. Cette situation risque de compromettre 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 européenne.

(3) On constate une tendance à la perpétration d'attaques à grande échelle de plus en plus dangereuses et régulières contre des systèmes d'information critiques pour les États ou certaines fonctions du secteur public ou privé. Parallèlement, des outils de plus en plus sophistiqués sont mis au point, lesquels peuvent être utilisés par des criminels pour lancer des cyberattaques de divers types.

[17] JO C […] du […], p. […].

(4) Il importe d'arrêter des définitions communes dans ce domaine, notamment pour les systèmes d'information et les données informatiques, de manière à garantir l'application cohérente de la présente directive dans tous les États membres.

(5) Il convient d'adopter une position commune sur les éléments constitutifs des infractions pénales en créant les infractions communes d'accès illicite à un système d'information, d'atteinte à l'intégrité d'un système, d'atteinte à l'intégrité des données et d'interception illégale de données.

(6) Il conviendrait que les États membres prévoient des sanctions pour réprimer les attaques contre les systèmes d'information. Les sanctions ainsi fixées devraient être effectives, proportionnées et dissuasives.

(7) Il y a lieu de prévoir des sanctions plus sévères en cas d'attaques contre un système d'information commises 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[18], si l'attaque est menée à grande échelle ou si, pour commettre l'infraction, l'identité réelle de l'auteur de ladite infraction est dissimulée, le titulaire légitime de l'identité étant ainsi lésé. Il y a également lieu de prévoir des sanctions plus sévères lorsqu'une telle attaque a causé un préjudice grave ou a porté atteinte à des intérêts essentiels.

(8) Dans ses conclusions des 27 et 28 novembre 2008, le Conseil a invité les États membres et la Commission à définir une nouvelle stratégie, en prenant en considération le contenu de la convention du Conseil de l'Europe sur la cybercriminalité de 2001. Cette convention est le cadre juridique de référence de la lutte contre la cybercriminalité, y compris les attaques contre les systèmes d'information, et la présente directive s'en inspire.

(9) 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 énumérées dans la présente directive. On entend par «outils», par exemple, des maliciels, notamment des réseaux zombies, utilisés pour lancer des cyberattaques.

(10) La présente directive n'a pas pour objet d'engager la responsabilité pénale en l'absence d'intention délictueuse, notamment dans le cas d'interventions visant à tester ou à protéger un système d'information après en avoir obtenu l'autorisation.

(11) 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 dont les points de contact sont disponibles vingt-quatre heures sur vingt-quatre et sept jours sur sept pour échanger des informations afin de garantir une assistance immédiate aux enquêtes ou procédures portant sur des infractions pénales liées à des données et des systèmes d'information, ou pour recueillir des preuves électroniques d'une infraction pénale. Compte tenu de la rapidité avec laquelle des attaques à grande échelle peuvent être menées, il conviendrait que tous les États membres soient en mesure de répondre promptement aux demandes urgentes émanant de ce réseau de points de contact. L'assistance

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

demandée devrait notamment consister à faciliter ou à exécuter directement des mesures telles que la fourniture de conseils techniques, la conservation des données, la collecte de preuves, la communication d'informations juridiques et la localisation de suspects.

(12) Il est nécessaire de recueillir des données sur les infractions relevant de la présente directive pour avoir une vision plus complète du problème au niveau de l'Union et permettre ainsi de formuler des réponses plus efficaces. Grâce aux données recueillies, des agences spécialisées comme Europol et l'Agence européenne chargée de la sécurité des réseaux et de l'information pourront mieux évaluer l'ampleur de la cybercriminalité et le niveau de sécurité des réseaux et de l'information en Europe.

(13) L'existence de lacunes et de différences importantes dans les législations nationales en matière d'attaques contre des 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 sans frontières, les attaques lancées contre eux ont une dimension transfrontière qui met en lumière la nécessité de prendre d'urgence des mesures complémentaires pour harmoniser le droit pénal dans ce domaine. Par ailleurs, il convient de faciliter la coordination des poursuites judiciaires en cas d'attaque contre des systèmes d'information par l'adoption de la décision-cadre 2009/948/JAI du Conseil relative à la prévention et au règlement des conflits en matière d'exercice de la compétence dans le cadre des procédures pénales.

(14) Étant donné que les objectifs de la présente directive, à savoir garantir que les attaques contre des systèmes d'information soient passibles, dans tous les États membres, de sanctions pénales effectives, proportionnées et dissuasives, et améliorer et favoriser la coopération judiciaire en supprimant les complications potentielles, ne peuvent être réalisés de manière suffisante par les États membres, puisque les règles doivent être communes et compatibles, et que lesdits objectifs peuvent donc être mieux réalisés au niveau de l'Union européenne, celle-ci peut adopter des mesures, conformément au principe de subsidiarité visé à l'article 5 du traité sur l'Union européenne. La présente directive n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

(15) Tout traitement de données à caractère personnel réalisé aux fins de l'application de la présente directive devrait être conforme aux dispositions de la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel dans le cadre de la coopération policière et judiciaire en matière pénale[19], pour les activités de traitement relevant de son champ d'application et du règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données[20].

(16) La présente directive respecte les droits fondamentaux et est conforme aux principes consacrés en particulier par la Charte des droits fondamentaux de l'Union européenne, notamment la protection des données à caractère personnel, la liberté d'expression et

---

19 JO L 350 du 30.12.2008, p. 60.

20 JO L 8 du 12.1.2001, p. 1.

d'information, le droit à un procès équitable, la présomption d'innocence et le droit à la défense, ainsi qu'aux 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 transposée en conséquence.

(17) [Conformément aux articles 1er, 2, 3 et 4 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 le fonctionnement de l'Union européenne, le Royaume-Uni et l'Irlande ont notifié leur souhait de participer à l'adoption et à l'application de la présente directive] OU [Sans préjudice de l'article 4 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, le Royaume-Uni et l'Irlande ne participeront pas à l'adoption de la présente directive et ne seront donc pas liés par celle-ci ni soumis à son application].

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

ONT ADOPTÉ LA PRÉSENTE DIRECTIVE:

Article premier

Objet

La présente directive définit des infractions pénales en matière d'attaques contre les systèmes d'information et instaure des règles minimales pour l'établissement des peines sanctionnant ces infractions. Elle vise également à mettre en place des dispositifs communs pour prévenir ces attaques et améliorer la coopération judiciaire européenne dans ce domaine.

Article 2

Définitions

Aux fins de la présente directive, on entend par:

a) «système d'information»: tout dispositif isolé ou groupe de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, conformément à un programme, un traitement automatisé de données informatiques, ainsi que les données informatiques stockées, traitées, récupérées ou transmises par ces derniers en vue de leur fonctionnement, utilisation, protection et maintenance;

b) «données informatiques»: toute représentation de faits, d'informations ou de notions sous une forme susceptible d'être traitée par un système d'information, y compris un programme permettant à ce dernier d'exécuter une fonction;

c) «personne morale»: toute entité à laquelle le droit en vigueur reconnaît ce statut, à l'exception des États et des autres entités publiques dans l'exercice de prérogatives de puissance publique, et des organisations internationales relevant du droit public;

d) «sans en avoir le droit»: un accès ou une atteinte à l'intégrité non autorisé(e) par le propriétaire ou autre détenteur de droits au système ou à une partie du système, ou non prévu(e) par la législation nationale.

Article 3

Accès illicite à des systèmes d'information

. Les États membres prennent les mesures nécessaires pour faire en sorte que l'accès intentionnel, sans en avoir le droit, à tout ou partie d'un système d'information devienne une infraction pénale punissable, au moins dans les cas où les faits ne sont pas sans gravité.

Article 4

Atteinte à l'intégrité d'un système

Les États membres prennent les mesures nécessaires pour faire en sorte que le fait de provoquer intentionnellement une perturbation grave ou une interruption du fonctionnement d'un système d'information, en introduisant, transmettant, endommageant, effaçant, détériorant, modifiant, supprimant ou rendant inaccessibles des données informatiques devienne une infraction pénale punissable lorsque l'acte est commis sans que l'auteur en ait le droit, au moins dans les cas où les faits ne sont pas sans gravité.

Article 5

Atteinte à l'intégrité des données

Les États membres prennent les mesures nécessaires pour faire en sorte que le fait d'effacer, d'endommager, de détériorer, de modifier, de supprimer ou de rendre inaccessibles des données informatiques d'un système d'information de manière intentionnelle devienne une infraction pénale punissable lorsque l'acte est commis sans que l'auteur en ait le droit, au moins dans les cas où les faits ne sont pas sans gravité.

Article 6

Interception illégale

Les États membres prennent les mesures nécessaires pour faire en sorte que l'interception intentionnelle, par des moyens techniques, de transmissions non publiques de données informatiques vers un système d'information ou à partir ou à l'intérieur d'un tel système, y compris d'émissions électromagnétiques à partir d'un système d'information contenant des données informatiques, devienne une infraction pénale punissable si l'auteur la commet sans en avoir le droit.

Article 7

Outils utilisés pour commettre les infractions

Les États membres prennent les mesures nécessaires pour faire en sorte que la production, la vente, l'acquisition en vue de l'utilisation, l'importation, la possession, la distribution ou la mise à disposition d'une autre manière des éléments ci-dessous devienne une infraction pénale punissable si elle est commise intentionnellement et sans en avoir le droit, dans le but de commettre l'une des infractions visées aux articles 3 à 6:

a) un dispositif, notamment un programme informatique, essentiellement conçu ou adapté aux fins de commettre l'une des infractions visées aux articles 3 à 6;

b) le mot de passe d'un ordinateur, un code d'accès ou des données de même nature grâce auxquelles il est possible d'accéder à tout ou partie d'un système d'information.

Article 8

Incitation et complicité et tentative

1. Les États membres font en sorte que le fait d’inciter à commettre l’une des infractions visées aux articles 3 à 7 et de s’en rendre complice devienne une infraction pénale punissable.

2. Les États membres font en sorte que la tentative de commettre les infractions visées aux articles 3 à 6 devienne une infraction pénale punissable.

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.

Article 10

Circonstances aggravantes

1. 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 cinq ans lorsqu’elles sont commises dans le cadre d’une organisation criminelle au sens de la décision-cadre 2008/841/JAI.

2. Les États membres prennent les mesures nécessaires pour faire en sorte que les infractions visées aux articles 3 à 6 soient passibles d’une peine d’emprisonnement

maximale d’au moins cinq ans lorsqu’elles sont commises au moyen d'un outil conçu pour lancer des attaques contre un nombre important de systèmes d'information ou des attaques causant un préjudice considérable, tel que la perturbation de services de réseau, des coûts financiers ou la perte de données à caractère personnel.

3. Les États membres prennent les mesures nécessaires pour faire en sorte que les infractions visées aux articles 3 à 6 soient passibles d’une peine d’emprisonnement maximale d’au moins cinq ans si, pour les commettre, leur auteur a dissimulé son identité réelle, causant ainsi un préjudice au titulaire légitime de l'identité.

Article 11

Responsabilité des personnes morales

1. Les États membres prennent les mesures nécessaires pour faire en sorte que les personnes morales puissent être tenues pour responsables des infractions visées aux articles 3 à 7, commises à leur profit par toute personne agissant soit individuellement soit en tant que membre d’un organe de la personne morale, et exerçant un pouvoir de direction en son sein à l’un des titres suivants:

a) un mandat de représentation de la personne morale;

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

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

2. Les États membres prennent les mesures nécessaires pour faire en sorte que les personnes morales puissent être tenues responsables lorsqu’un défaut de surveillance ou de contrôle imputable à une personne visée au paragraphe 1 a rendu possible la commission, par une personne placée sous son autorité, de l'une des infractions visées aux articles 3 à 8 au profit de cette personne morale.

3. La responsabilité des personnes morales au titre des paragraphes 1 et 2 n'exclut pas les poursuites pénales contre les personnes physiques auteurs ou complices d'une des infractions énoncées aux articles 3 à 8.

Article 12

Sanctions contre les personnes morales

1. Les États membres prennent les mesures nécessaires pour faire en sorte qu’une personne morale déclarée responsable au titre de l’article 11, paragraphe 1, soit passible de peines effectives, proportionnées et dissuasives, qui comprennent des amendes pénales et 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 contrôle judiciaire;

d) une mesure judiciaire de dissolution;

e) la fermeture temporaire ou permanente d'établissements qui ont servi à commettre l'infraction.

2. Les États membres prennent les mesures nécessaires pour faire en sorte qu'une personne morale dont la responsabilité est engagée au titre de l'article 11, paragraphe 2, soit passible de peines ou de mesures effectives, proportionnées et dissuasives.

Article 13

Compétence

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

a) en tout ou en partie sur le territoire de l'État membre concerné; ou

b) par l'un de leurs ressortissants ou une personne qui a sa résidence habituelle sur le territoire de l'État membre concerné; or

c) au profit d'une personne morale dont le siège est situé sur le territoire de l'État membre concerné.

2. Lorsqu'ils établissent leur compétence conformément au paragraphe 1, point a), les États membres font en sorte qu'elle comprenne les cas où:

a) l'auteur de l'infraction l'a commise alors qu'il était physiquement présent sur le territoire de l'État membre concerné, même si l'infraction ne vise pas un système d'information situé sur son territoire; ou

b) l'infraction vise un système d'information situé sur le territoire de l'État membre concerné, même si l'auteur de l'infraction n'était pas physiquement présent sur son territoire lors de la commission de l'infraction.

Article 14

Échange d'informations

1. Aux fins de l'échange d'informations relatives aux infractions visées aux articles 3 à 8, et conformément aux règles régissant la protection des données, les États membres recourent 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 pour pouvoir répondre à des demandes urgences dans un délai maximal de huit heures. La réponse doit au moins préciser si la demande d'aide sera satisfaite, sous quelle forme et dans quel délai.

2. Les États membres communiquent à la Commission le point de contact qu'ils ont désigné aux fins de l'échange d'informations sur les infractions visées aux articles 3 à 8. La Commission transmet ces informations aux autres États membres.

Article 15

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 8.

2. Les statistiques visées au paragraphe 1 portent, au minimum, sur le nombre d'infractions visées aux articles 3 à 8 qui sont signalées aux États membres, ainsi que sur la suite donnée à ces signalements; elles mentionnent, pour chaque année, le nombre de cas signalés qui ont fait l'objet d'une enquête, le nombre de personnes poursuivies et le nombre de personnes condamnées pour les infractions visées aux articles 3 à 8.

3. Les États membres transmettent à la Commission les données recueillies conformément au présent article. Ils veillent aussi à ce qu'un état consolidé de ces rapports statistiques soit publié.

Article 16

Abrogation de la décision-cadre 2005/222/JAI

La décision-cadre 2005/222/JAI est abrogée, sans préjudice des obligations des États membres relatives aux délais de transposition en droit interne.
Les références faites à la décision-cadre abrogée s’entendent comme faites à la présente directive.

Article 17

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 [deux ans après son adoption]. Ils communiquent immédiatement à la Commission le texte de ces dispositions ainsi qu'un tableau de correspondance entre ces dispositions et la présente directive. 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.

2. Les États membres communiquent à la Commission le texte des principales dispositions de droit interne qu'ils adoptent dans le domaine régi par la présente directive.

Article 18

Rapports

1. Au plus tard le [QUATRE ANS À COMPTER DE L'ADOPTION] et ensuite tous les trois ans, la Commission présente au Parlement européen et au Conseil un rapport sur l'application de la présente directive dans les États membres, qui comprend toute proposition nécessaire.

2. Les États membres transmettent à la Commission toutes les informations nécessaires à l'élaboration du rapport visé au paragraphe 1. Ces informations contiennent une description détaillée des mesures législatives et non législatives adoptées pour transposer la présente directive.

Article 19

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 20

Destinataires

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

Fait à Bruxelles, le

Par le Parlement européen	*Par le Conseil*
Le Président	*Le Président*