(Actes adoptés en application du titre VI du traité sur l'Union européenne)

DÉCISION-CADRE 2005/222/JAI DU CONSEIL

du 24 février 2005

relative aux attaques visant les systèmes d'information

LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur l'Union européenne, et notamment son article 29, son article 30, paragraphe 1, point a), son article 31, paragraphe 1, point e), et son article 34, paragraphe 2, point b),

vu la proposition de la Commission,

vu l'avis du Parlement européen [1],

considérant ce qui suit:

(1) La présente décision-cadre vise 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.

(2) Il a été constaté que les systèmes d'information font l'objet d'attaques, notamment dues à la criminalité organisée, et que l'inquiétude croît face à l'éventualité d'attaques terroristes contre les systèmes d'information qui font partie de l'infrastructure critique des États membres. 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) Une réponse efficace à ces menaces suppose une approche d'ensemble en matière de sécurité des réseaux et de l'information, comme l'ont souligné le plan d'action européen, la communication de la Commission intitulée «Sécurité des réseaux et de l'information: Proposition pour une approche politique européenne» et la résolution du Conseil du 28 janvier 2002 relative à une approche commune et à des actions spécifiques dans le domaine de la sécurité des réseaux et de l'information [2].

(4) La nécessité de renforcer la prise de conscience des problèmes liés à la sécurité de l'information et de fournir une assistance pratique a également été soulignée par la résolution du Parlement européen du 5 septembre 2001.

(5) Les vides juridiques et les différences considérables présentées par les législations des États membres dans ce domaine peuvent freiner la lutte contre la criminalité organisée et le terrorisme et peuvent compliquer une coopération policière et judiciaire efficace en cas d'attaques contre les systèmes d'information. Les systèmes d'information modernes étant transnationaux et ne connaissant pas de frontières, ces attaques ont souvent une dimension transfrontière, et mettent ainsi en lumière le besoin urgent de poursuivre le rapprochement des droits pénaux dans ce domaine.

(6) Le plan d'action du Conseil et de la Commission concernant les modalités optimales de mise en œuvre des dispositions du traité d'Amsterdam relatives à l'établissement d'un espace de liberté, de sécurité et de justice [3], le Conseil européen de Tampere des 15 et 16 octobre 1999, le Conseil européen de Santa Maria da Feira des 19 et 20 juin 2000, la Commission dans son tableau de bord, et le Parlement européen dans sa résolution du 19 mai 2000 mentionnent ou préconisent des mesures législatives contre la criminalité utilisant les technologies avancées, notamment des définitions, des incriminations et des sanctions communes.

(7) Il est nécessaire de compléter le travail réalisé par les organisations internationales, plus particulièrement celui du Conseil de l'Europe sur le rapprochement du droit pénal et les travaux du G8 sur la coopération transnationale dans le domaine de la criminalité utilisant les technologies avancées, en proposant une approche commune dans ce domaine au niveau de l'Union européenne. Cet appel a été plus amplement développé dans la communication que la Commission a adressée au Conseil, au Parlement européen, au Comité économique et social européen et au Comité des régions, intitulée «Créer une société de l'information plus sûre en renforçant la sécurité des infrastructures de l'information et en luttant contre la cybercriminalité.»

(8) Les règles du droit pénal relatives aux attaques contre les systèmes d'information devraient être rapprochées pour garantir la meilleure coopération policière et judiciaire possible en ce qui concerne les infractions liées à ce type d'attaques et contribuer à la lutte contre la criminalité organisée et le terrorisme.

[1] JO C 300 E du 11.12.2003, p. 26.
[2] JO C 43 du 16.2.2002, p. 2.
[3] JO C 19 du 23.1.1999, p. 1.

(9) Tous les États membres ont ratifié la convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Les données à caractère personnel traitées dans le contexte de la mise en œuvre de la présente décision-cadre devraient être protégées conformément aux principes établis par ladite convention.

(10) Des définitions communes dans ce domaine, plus particulièrement pour les systèmes d'information et les données informatiques, sont indispensables pour assurer l'application cohérente de la présente décision-cadre dans les États membres.

(11) Il est nécessaire d'adopter une approche commune pour les éléments constitutifs des infractions pénales, en instituant des délits communs: accès illicite à un système d'information, atteinte à l'intégrité d'un système et atteinte à l'intégrité des données.

(12) Afin de lutter contre la criminalité liée à l'informatique, les États membres devraient assurer une coopération judiciaire efficace en ce qui concerne les infractions fondées sur les types de comportement visés aux articles 2, 3, 4 et 5.

(13) Il importe d'éviter la surincrimination, notamment pour les affaires mineures, de même que l'incrimination de détenteurs de droits et de personnes autorisées.

(14) Il est nécessaire que les États membres prévoient des sanctions pour réprimer les attaques contre les systèmes d'information. Ces sanctions sont efficaces, proportionnées et dissuasives.

(15) Il est pertinent de prévoir des peines plus sévères lorsqu'une attaque contre un système d'information est lancée dans le cadre d'une organisation criminelle telle que définie dans l'action commune 98/733/JAI du Conseil du 21 décembre 1998 relative à l'incrimination de la participation à une organisation criminelle dans les États membres de l'Union européenne [1]. Il convient également de prévoir des peines plus sévères lorsqu'une telle attaque a causé un préjudice grave ou a porté atteinte à des intérêts essentiels.

(16) Des mesures de coopération entre les États membres devraient également être envisagées, afin d'assurer une action efficace contre les attaques visant les systèmes d'information. Les États membres devraient par conséquent avoir recours, aux fins de l'échange d'informations, au réseau existant de points de contact opérationnels visés dans la recommandation du Conseil du 25 juin 2001 concernant les points de contact assurant un service vingt-quatre heures sur vingt-quatre pour lutter contre la criminalité liée à la haute technologie [2].

(17) Étant donné que les objectifs de la présente décision-cadre, à savoir garantir que des 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 CE. Conformément au principe de proportionnalité tel qu'énoncé audit article, la présente décision-cadre n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

(18) La présente décision-cadre respecte les droits fondamentaux et les principes reconnus à l'article 6 du traité sur l'Union européenne et reflétés dans la charte des droits fondamentaux de l'Union européenne, notamment ses chapitres II et VI,

A ARRÊTÉ LA PRÉSENTE DÉCISION-CADRE:

Article premier

Définitions

Aux fins de la présente décision-cadre, 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;

[1] JO L 351 du 29.12.1998, p. 1.

[2] JO C 187 du 3.7.2001, p. 5.

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 2

Accès illicite à des systèmes d'information

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

2. Les États membres peuvent décider que le comportement visé au paragraphe 1 ne soit érigé en infraction pénale qu'en cas d'infraction à une mesure de sécurité.

Article 3

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 4

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 5

Incitation, aide et complicité et tentative

1. Les États membres prennent les mesures nécessaires pour que soit rendu punissable le fait d'inciter ou d'aider à commettre l'une des infractions visées aux articles 2, 3 et 4 et de s'en rendre complice.

2. Les États membres font en sorte que la tentative de commettre les infractions visées aux articles 2, 3 et 4 soit punissable.

3. Les États membres peuvent décider de ne pas faire appliquer le paragraphe 2 en ce qui concerne les infractions visées à l'article 2.

Article 6

Sanctions

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

Article 7

Circonstances aggravantes

1. Les États membres prennent les mesures nécessaires pour faire en sorte que l'infraction visée à l'article 2, paragraphe 2, et celle visée aux articles 3 et 4 soient passibles d'une peine d'emprisonnement maximale d'au moins deux à cinq ans lorsqu'elles sont commises dans le cadre d'une organisation criminelle au sens de l'action commune 98/733/JAI, indépendamment de la peine qui y est visée.

2. Un État membre peut également prendre les mesures visées au paragraphe 1 lorsque l'infraction en question a causé un préjudice grave ou a porté atteinte à des intérêts essentiels.

Article 8

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 2, 3, 4 et 5, commises à leur profit par toute personne agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein sur l'une des bases suivantes:

a) un pouvoir de représentation de la personne morale, ou

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

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

2. Outre les cas prévus au paragraphe 1, les États membres font en sorte qu'une personne morale puisse être tenue responsable lorsqu'un défaut de surveillance ou de contrôle imputable à une personne visée au paragraphe 1 a rendu possible la commission des infractions visées aux articles 2, 3, 4 et 5 au profit de cette personne morale par une personne placée sous son autorité.

3. La responsabilité d'une personne morale au titre des paragraphes 1 et 2 n'exclut pas les poursuites pénales contre les personnes physiques auteurs, instigatrices ou complices de la commission des infractions visées aux articles 2, 3, 4 et 5.

Article 9

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 8, 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) des mesures d'exclusion du bénéfice d'un avantage ou d'une aide publics;

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

c) un placement sous contrôle judiciaire, ou

d) une mesure judiciaire de dissolution.

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 8, paragraphe 2, soit passible de peines et de mesures effectives, proportionnées et dissuasives.

Article 10

Compétence

1. Les États membres établissent leur compétence pour les infractions visées aux articles 2, 3, 4 et 5, lorsque l'infraction a été commise:

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

b) par l'un de leurs ressortissants, ou

c) au profit d'une personne morale dont le siège est situé sur leur territoire.

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 son territoire, 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 son territoire, même si l'auteur de l'infraction n'était pas physiquement présent sur ce territoire.

3. Lorsqu'en vertu de sa législation, un État membre ne procède pas encore à l'extradition ou à la remise de ses propres ressortissants, il prend les mesures nécessaires en vue d'établir sa compétence à l'égard des infractions visées aux articles 2, 3, 4 et 5 et d'en poursuivre l'auteur, le cas échéant, lorsqu'elles sont commises par l'un de ses ressortissants en dehors de son territoire.

4. Lorsqu'une infraction relève de la compétence de plusieurs États membres et que chacun d'eux peut valablement engager des poursuites sur la base des mêmes faits, les États membres concernés coopèrent pour décider lequel d'entre eux poursuivra les auteurs de l'infraction en vue, si possible, de centraliser la procédure dans un seul d'entre eux. À cette fin, les États membres peuvent avoir recours à tout organe ou mécanisme établi au sein de l'Union européenne pour faciliter la coopération entre leurs autorités judiciaires et la coordination de leurs actions. Pourront être pris en compte, successivement, les éléments de rattachement suivants:

— l'État membre est celui sur le territoire duquel les infractions ont été commises, conformément à l'article 10, paragraphe 1, point a), et paragraphe 2,

— l'État membre est celui dont l'auteur est un ressortissant,

— l'État membre est celui dans lequel l'auteur a été découvert.

5. Un État membre peut décider de ne pas appliquer la règle de compétence énoncée au paragraphe 1, points b) et c), ou de ne l'appliquer qu'à des situations ou des circonstances particulières.

6. Lorsqu'ils décident d'appliquer le paragraphe 5, les États membres en informent le secrétariat général du Conseil et la Commission en précisant, le cas échéant, les situations ou circonstances particulières dans lesquelles s'applique la décision.

Article 11

Échange d'informations

1. Aux fins de l'échange d'informations relatives aux infractions visées aux articles 2, 3, 4 et 5, et conformément aux règles régissant la protection des données, les États membres veillent à recourir au réseau existant de points de contact opérationnels, disponibles vingt-quatre heures sur vingt-quatre et sept jours sur sept.

2. Chaque État membre communique au secrétariat général du Conseil et à la Commission le nom des points de contact désignés aux fins de l'échange d'informations sur les infractions relatives aux attaques contre les systèmes d'information. Le secrétariat général transmet ces informations aux autres États membres.

Article 12

Mise en œuvre

1. Les États membres adoptent au plus tard le 16 mars 2007 les mesures nécessaires pour se conformer aux dispositions de la présente décision-cadre.

2. Pour le 16 mars 2007, les États membres communiquent au secrétariat général du Conseil et à la Commission le texte des dispositions transposant dans leur droit national les obligations qui leur incombent en vertu de la présente décision-cadre. Pour le 16 septembre 2007, sur la base d'un rapport établi à partir des informations recueillies et d'un rapport de la Commission, le Conseil vérifie dans quelle mesure les États membres ont pris les mesures nécessaires pour se conformer à la présente décision-cadre.

Article 13

Entrée en vigueur

La présente décision-cadre entre en vigueur le jour de sa publication au *Journal officiel de l'Union européenne*.

Fait à Bruxelles, le 24 février 2005.

Par le Conseil

Le président

N. SCHMIT