Informations de base

2002/0086(CNS) CNS - Procédure de consultation Décision	Procédure terminée
Coopération judiciaire pénale: attaques visant les réseaux de communication et les systèmes d'information. Décision-cadre Abrogation 2010/0273(COD) **Subject** 3.30.25 Réseaux mondiaux et société de l'information, internet 7.40.04 Coopération judiciaire en matière pénale	

Acteurs principaux

Parlement européen

Commission au fond	Rapporteur(e)	Date de nomination
LIBE Libertés et droits des citoyens, justice, affaires intérieures	CEDERSCHIÖLD Charlotte (PPE-DE)	23/05/2002

Commission pour avis	Rapporteur(e) pour avis	Date de nomination
JURI Juridique et marché intérieur	La commission a décidé de ne pas donner d'avis.	
ITRE Industrie, commerce extérieur, recherche, énergie	CAPPATO Marco (NI)	04/06/2002

Conseil de l'Union européenne

Formation du Conseil	Réunions	Date
Justice et affaires intérieures(JAI)	2489	2003-02-27
Justice et affaires intérieures(JAI)	2642	2005-02-24

Commission européenne

DG de la Commission	Commissaire
Justice et consommateurs	

Evénements clés

Date	Evénement	Référence	Résumé
19/04/2002	Publication de la proposition législative	COM(2002)0173	Résumé

13/06/2002	Annonce en plénière de la saisine de la commission		
02/10/2002	Vote en commission		Résumé
02/10/2002	Dépôt du rapport de la commission, 1ère lecture/lecture unique	A5-0328/2002	
21/10/2002	Débat en plénière		
22/10/2002	Décision du Parlement	T5-0495/2002	Résumé
27/02/2003	Débat au Conseil		Résumé
24/02/2005	Adoption de l'acte par le Conseil suite à la consultation du Parlement		
24/02/2005	Fin de la procédure au Parlement		
16/03/2005	Publication de l'acte final au Journal officiel		

Informations techniques

Référence de la procédure	2002/0086(CNS)
Type de procédure	CNS - Procédure de consultation
Sous-type de procédure	Note thématique
Instrument législatif	Décision
Modifications et abrogations	Abrogation 2010/0273(COD)
Base juridique	Traité sur l'Union européenne (après Amsterdam) M 029 Traité sur l'Union européenne (après Amsterdam) M 034-p2 Traité sur l'Union européenne (après Amsterdam) M 031 Traité sur l'Union européenne (après Amsterdam) M 030-p1
État de la procédure	Procédure terminée
Dossier de la commission	LIBE/5/16198

Portail de documentation

Parlement Européen

Type de document	Commission	Référence	Date	Résumé
Rapport déposé de la commission, 1ère lecture/lecture unique		A5-0328/2002	02/10/2002	
Texte adopté du Parlement, 1ère lecture/lecture unique		T5-0495/2002 JO C 300 11.12.2003, p. 0026-0152 E	22/10/2002	Résumé

Commission Européenne

Type de document	Référence	Date	Résumé
Document de base législatif	COM(2002)0173 JO C 203 27.08.2002, p. 0109 E	19/04/2002	Résumé

Informations complémentaires		
Source	**Document**	**Date**
Commission européenne	EUR-Lex	

Acte final	
Acte Justice et affaires intérieures 2005/0222 JO L 069 16.03.2005, p. 0067-0071	Résumé

Coopération judiciaire pénale: attaques visant les réseaux de communication et les systèmes d'information. Décision-cadre

2002/0086(CNS) - 27/02/2003

Le Conseil, moyennant un certain nombre de réserves d'examen parlementaire et sans préjudice de l'examen de l'avis du Parlement européen, a dégagé une approche commune sur la décision-cadre relative aux attaques visant les systèmes d'information. Le Conseil estime qu'il s'agit là d'un instrument très important car on redoute de plus en plus que des bandes criminelles organisées n'utilisent les réseaux de communication pour lancer des attaques contre les systèmes d'information à leurs propres fins. Il a notamment été constaté que les systèmes d'information faisaient l'objet d'attaques de la part la criminalité organisée, et que l'inquiétude croissait 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 (ELSJ), et appelle donc une réaction au niveau de l'Union européenne. Les vides juridiques et les différences considérables présentées par les législations des États membres dans ce domaine freinent la lutte contre la criminalité organisée et le terrorisme, et font obstacle à une coopération policière et judiciaire efficace en cas d'attaques contre les systèmes d'information. Les réseaux de télécommunication électroniques modernes étant transnationaux et ne connaissant pas de frontières, ces attaques ont souvent une dimension internationale, et mettent ainsi en lumière le besoin urgent de poursuivre le rapprochement des droits pénaux dans ce domaine. La présente décision-cadre exige des États membres qu'ils érigent en infraction pénale l'accès illicite aux systèmes d'information. Elle prévoit en outre des sanctions efficaces, proportionnées et dissuasives pour réprimer les attaques contre les systèmes d'information, y compris des peines d'emprisonnement dans les cas graves.

Coopération judiciaire pénale: attaques visant les réseaux de communication et les systèmes d'information. Décision-cadre

2002/0086(CNS) - 19/04/2002 - Document de base législatif

OBJECTIF : rapprocher les règles pénales des États membres réprimant les attaques contre les systèmes d'information, afin notamment de contribuer à la lutte contre la criminalité organisée et le terrorisme, et renforcer la coopération judiciaire dans le domaine des infractions pénales liées aux attaques contre les systèmes d'information. CONTENU : les attaques contre les systèmes d'information constituent une menace pour la réalisation d'une société de l'information plus sûre et d'un espace de liberté, de sécurité et de justice (ELSJ). En vue de répondre à cette menace, la présente proposition de décision-cadre a pour objet de rapprocher les législations et les réglementations des États membres en matière de coopération policière et judiciaire pénale. Elle prévoit des règles minimales relatives aux éléments constitutifs des infractions pénales, tout particulièrement dans le domaine de la criminalité organisée et du terrorisme. Elle vise également à assurer la compatibilité des règles applicables dans les États membres en vue de faciliter et d'accélérer la coopération entre les autorités judiciaires. Aux fins de la présente proposition, les systèmes d'information couvrent les ordinateurs personnels autonomes, les agendas électroniques personnels, les téléphones mobiles, les intranets, les extranets, ainsi que les réseaux, serveurs et autres infrastructures d'Internet. L'intention n'est pas d'exiger que les États membres criminalisent des actes mineurs ou insignifiants. Seuls sont visés les actes graves. En particulier, la proposition n'affecte pas les droits à la vie privée ou à la protection des données et les obligations prévues par le droit communautaire (directives 95/46/CE et 97/66/CE, par exemple). Par conséquent, la proposition couvre uniquement les actes suivants : - accès non autorisé à des systèmes d'information. Cela couvre la notion de piratage qui consiste à accéder sans y être autorisé à un ordinateur ou à un réseau d'ordinateurs; - perturbation de systèmes d'information. L'un des moyens les plus connus de dégrader les services offerts sur Internet ou d'en dénier l'accès est une attaque par "déni de service" (DdS) visant à submerger les serveurs ou les fournisseurs de services Internet de messages générés automatiquement; - exécution de logiciels malveillants modifiant ou détruisant des données (virus). - interception malveillante des communications ("sniffing" ou reniflage); - présentation mensongère (l'usurpation de l'identité ou de l'adresse d'une autre personne sur Internet et son utilisation à des fins malveillantes, appelé "spoofing"). La proposition ne couvre pas seulement les actes visant les États membres. Elle s'applique également à des actes perpétrés sur le territoire de l'Union européenne et visant des systèmes d'information situés sur le territoire de pays tiers. Le rapprochement au niveau de l'Union devra tenir compte des travaux réalisés dans les enceintes internationales et s'inscrire dans la ligne des politiques communautaires actuelles. La proposition devrait permetre un rapprochement plus poussé des législations au sein de l'Union que cela n'aété possible dans d'autres enceintes internationales.

Coopération judiciaire pénale: attaques visant les réseaux de communication et les systèmes d'information. Décision-cadre

2002/0086(CNS) - 22/10/2002 - Texte adopté du Parlement, 1ère lecture/lecture unique

En adoptant le rapport de Mme Charlotte CEDERSCHIÖLD (PPE-DE, S), le Parlement européen a approuvé la proposition de décision-cadre du Conseil sous réserve d'amendements. Le Parlement insiste sur la nécessité d'adopter d'urgence, au titre du troisième pilier, un instrument de l'Union européenne visant à la protection des données à caractère personnel tout particulièrement à l'égard des services chargés de l'application de la loi. Par ailleurs, la décision-cadre devrait respecter les droits et les libertés fondamentaux et les principes reconnus non seulement par la Charte des droits fondamentaux de l'Union européenne, mais aussi par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et par la jurisprudence de la Cour européenne des droits de l'homme et par le droit national et le droit international en matière de droits de l'homme et de libertés fondamentales. En conséquence, la présente décision-cadre et les mesures nationales prises pour transposer celle-ci ne pourront servir à réprimer la liberté d'opinion, d'expression, de manifestation et d'association. Le Parlement insiste également sur la prévention. À cette fin, les États membres devraient inciter les acteurs de la société de l'information à développer une culture de la sécurité, notamment grâce à des campagnes d'information menées avec les employeurs, les organisations et les autres acteurs concernés. La Commission est invitée à prendre des initiatives propres à sensibiliser davantage les citoyens, les entreprises et le secteur public aux risques pour les réseaux d'information. Enfin de l'avis du Parlement, les comportements qui, selon les législations nationales, sont considérés comme mineurs ou insignifiants, doivent être exclus de l'obligation d'appliquer des sanctions pénales et partant, du champ d'application de la présente décision-cadre.

Coopération judiciaire pénale: attaques visant les réseaux de communication et les systèmes d'information. Décision-cadre

2002/0086(CNS) - 24/02/2005 - Acte final

OBJECTIF : 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.

ACTE LÉGISLATIF : Décision-cadre 2005/222 JAI relative aux attaques visant des systèmes d'information.

CONTENU : étant donné que les systèmes d'information font l'objet d'attaques dues notamment à la criminalité organisée et que l'éventualité d'attaques terroristes contre les systèmes d'information qui font partie de l'infrastructure critique des États membres augmente, une réaction au niveau des États membres est nécessaire afin de ne pas compromettre la réalisation d'une société de l'information sûre et d'un espace de liberté, de sécurité et de justice.

Les vides juridiques et les différences considérables présentées par les législations des États membres dans ce domaine freinent la lutte contre la criminalité organisée et le terrorisme, et font obstacle à une coopération policière et judiciaire efficace en cas d'attaques contre les systèmes d'information. Les réseaux de télécommunication électroniques modernes étant transnationaux et ne connaissant pas de frontières, ces attaques ont souvent une dimension internationale, et mettent ainsi en lumière le besoin urgent de poursuivre le rapprochement des droits pénaux dans ce domaine.

La présente décision-cadre exige des États membres qu'ils érigent en infraction pénale l'accès illicite aux systèmes d'information. Elle prévoit en outre des sanctions efficaces, proportionnées et dissuasives pour réprimer les attaques contre les systèmes d'information, y compris des peines d'emprisonnement dans les cas graves.

Aux fins de l’échange d’informations relatives aux infractions, et conformément aux règles régissant la protection des données, les États membres veilleront à recourir au réseau existant de points de contact opérationnels, disponibles vingt-quatre heures sur vingt-quatre et sept jours sur sept.

ENTRÉE EN VIGUEUR: 16/03/2005.

TRANSPOSITION : 16/03/2007.