Informations de base

2001/2280(COS) COS - Procédure sur un document stratégique (historique) Communications électroniques: sécurité des réseaux et de l'information, rôle du secteur public **Subject** 1.20.09 Protection de la vie privée et des données 3.30.05 Communications électroniques et mobiles, services cryptés	Procédure terminée

Acteurs principaux

Parlement européen

Commission au fond	Rapporteur(e)	Date de nomination
LIBE Libertés et droits des citoyens, justice, affaires intérieures	PACIOTTI Elena Ornella (PSE)	10/10/2001

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	VAN VELZEN W.G. (PPE-DE)	22/11/2001
CULT Culture, jeunesse, éducation, médias et sports	La commission a décidé de ne pas donner d'avis.	

Conseil de l'Union européenne

Formation du Conseil	Réunions	Date
Affaires générales	2406	2002-01-28
Affaires économiques et financières ECOFIN	2485	2003-02-18
Transports, télécommunications et énergie	2374	2001-10-15
Transports, télécommunications et énergie	2472	2002-12-05

Commission européenne

DG de la Commission	Commissaire
Réseaux de communication, contenu et technologies	

Evénements clés

Date	Evénement	Référence	Résumé
06/06/2001	Publication du document de base non-législatif	COM(2001)0298	Résumé
15/10/2001	Débat au Conseil		
13/12/2001	Annonce en plénière de la saisine de la commission		
28/01/2002	Adoption de résolution/conclusions par le Conseil		
12/09/2002	Vote en commission		Résumé
12/09/2002	Dépôt du rapport de la commission	A5-0311/2002	
22/10/2002	Décision du Parlement	T5-0490/2002	Résumé
22/10/2002	Fin de la procédure au Parlement		
05/12/2002	Adoption de résolution/conclusions par le Conseil		
18/02/2003	Adoption de résolution/conclusions par le Conseil		
11/12/2003	Publication de l'acte final au Journal officiel		

Informations techniques	
Référence de la procédure	2001/2280(COS)
Type de procédure	COS - Procédure sur un document stratégique (historique)
Sous-type de procédure	Document stratégique de la Commission
Base juridique	Règlement du Parlement EP 148
État de la procédure	Procédure terminée
Dossier de la commission	LIBE/5/15587

Communications électroniques: sécurité des réseaux et de l'information, rôle du secteur public

2001/2280(COS) - 31/05/2006 - Document de suivi

Le but de la présente communication est de revitaliser la stratégie exposée par la Commission en 2001 dans le domaine de la **sécurité des réseaux et de l'information (SRI).** Elle examine l'état actuel des menaces pour la sécurité dans la société de l'information et détermine les mesures supplémentaires à prendre pour améliorer la SRI.

Tirant parti de l'expérience acquise par les États membres et au niveau de la Communauté européenne, la Commission propose une approche dynamique et intégrée qui rassemble toutes les parties concernées et qui repose sur le **dialogue**, le **partenariat** et la **responsabilisation**. Étant donné les rôles complémentaires des secteurs public et privé dans la création d'une culture de la sécurité, les initiatives politiques dans ce domaine doivent s' appuyer sur **un dialogue ouvert, inclusif et multipartite**.

Parmi les propositions spécifiques de la Commission figurent l'évaluation comparative des politiques nationales relatives à la sécurité des réseaux et de l'information pour améliorer le dialogue entre les pouvoirs publics, répertorier les meilleures pratiques et élever le niveau de sensibilisation à la sécurité parmi les utilisateurs finals. Un débat multipartite structuré sera engagé sur la façon d'exploiter au mieux les outils et les instruments réglementaires existants pour atteindre un équilibre entre la sécurité et la protection des droits fondamentaux, y compris la vie privée.

L'ENISA, l'Agence européenne chargée de la sécurité des réseaux et de l'information établie à Iraklion, en Grèce, sera chargée de mettre au point un cadre approprié pour la collecte de données afin de traiter les incidents de sécurité et les niveaux de confiance des consommateurs mesurés partout en Europe. L'ENISA sera également invitée à examiner la faisabilité d'un système européen de partage d'informations et d'alerte qui comportera un portail européen multilingue fournissant des informations sur les menaces, les risques et les alertes.

La Commission invitera les États membres, le secteur privé et la communauté de la recherche à créer un partenariat stratégique pour assurer la disponibilité des données sur le secteur de la sécurité des TIC et sur l'évolution des tendances du marché pour les produits et des services

correspondants dans l'UE.Enfin, les États membres et le secteur privé sont invités à jouer un rôle plus proactif et énergique dans l'amélioration de la sécurité des réseaux et de l'information.

La Commission fera rapport au Conseil et au Parlement européen au milieu de 2007 sur les activités entreprises, les premiers résultats et l'état d' avancement des différentes initiatives, y compris celles de l'ENISA et celles prises au niveau des États membres et dans le secteurprivé. Le cas échéant, elle proposera une recommandation concernant la sécurité des réseaux et de l'information.

Communications électroniques: sécurité des réseaux et de l'information, rôle du secteur public

2001/2280(COS) - 31/05/2006 - Document annexé à la procédure

Dans le droit fil de la communication de la Commission, destinée à revitaliser la stratégie de 2001 sur la «Sécurité des réseaux et de l'information » (voir résumé du 06/06/2001), le présent document examine l'état actuel des menaces pour la sécurité dans la société de l'information et détermine les mesures supplémentaires à prendre pour améliorer la sécurité des réseaux et de l'information (SRI).

Tirant parti de l'expérience acquise par les États membres et au niveau de la Communauté européenne, l'ambition est de développer, en Europe, une stratégie dynamique et globale basée sur une culture de sécurité et fondée sur le dialogue, le partenariat et la responsabilisation.

Le document s'articule autour de 2 axes :

1- les défis clés liés à l'amélioration de la sécurité de la société de l'information : une atteinte à la SRI (sécurité des réseaux et de l'information) peut avoir des conséquences qui dépassent sa dimension économique. En effet, la possibilité de voir les problèmes de sécurité décourager les utilisateurs et freiner l'adoption des TIC est une préoccupation constante dès lors que la disponibilité, la fiabilité et la sécurité sont des conditions indispensables pour garantir les droits fondamentaux en ligne.

En outre, en raison de la connectivité accrue des réseaux, d'autres infrastructures critiques (transport, énergie, etc.) deviennent également de plus en plus dépendantes de l'intégrité de leurs systèmes d'information respectifs.

Tant les entreprises que les citoyens d'Europe sous-estiment encore les risques. Différentes raisons en sont la cause, mais la plus importante semble être, pour les entreprises, la mauvaise perception du retour sur investissements dans la sécurité et, pour les citoyens, la méconnaissance de leur responsabilité dans la chaîne de sécurité globale.

2- la mise en place d'une approche dynamique de la sécurité d'une société de l'information : une société de l'information sûre doit être basée sur une SRI renforcée et une culture de la sécurité largement répandue. À cet effet, la Commission propose une approche dynamique et intégrée qui rassemble toutes les parties concernées et qui repose sur le dialogue, le partenariat et la responsabilisation. Étant donné les rôles complémentaires des secteurs public et privé dans la création d'une culture de la sécurité, les initiatives politiques dans ce domaine doivent s'appuyer sur un dialogue ouvert, inclusif et multipartite.

Cette approche, et les mesures associées, compléteront et enrichiront le plan de la Commission pour poursuivre le développement d'un cadre politique complet et dynamique par un certain nombre d'initiatives en 2006, à savoir :

1) aborder l'évolution du pourriel (« SPAM ») et d'autres menaces, comme les logiciels espions et d'autres formes de logiciel malveillant, dans une communication spécifique ;

2) faire des propositions visant à améliorer la coopération entre les autorités de police et à réprimer de nouvelles formes d'activité criminelle qui exploitent Internet et sapent le fonctionnement des infrastructures critiques ; cette thématique fera l'objet d'une communication spécifique sur la cybercriminalité.

En conclusion, la communication rappelle que le fait d'identifier et relever les défis à la sécurité des systèmes d'information et des réseaux dans l'UE exige l'engagement complet de toutes les parties prenantes. La démarche politique décrite dans la communication cherche à y parvenir en renforçant une approche multipartite. Cette approche se fonderait sur l'intérêt mutuel des parties, identifierait leurs rôles respectifs et développerait un cadre dynamique pour promouvoir l'élaboration de mesures publiques efficaces et des initiatives du secteur privé.

La Commission fera rapport au Conseil et au Parlement européen au milieu de 2007 sur les activités entreprises, les premiers résultats et l'état d' avancement des différentes initiatives, y compris celles de l'ENISA (Agence européenne chargée de la sécurité des réseaux et de l'information) et celles prises au niveau des États membres et dans le secteur privé. Le cas échéant, elle proposera une recommandation concernant la sécurité des réseaux et de l'information.

Communications électroniques: sécurité des réseaux et de l'information, rôle du secteur public

2001/2280(COS) - 06/06/2001 - Document de base non législatif

OBJECTIF : proposer une approche politique européenne en vue d'accroître la sécurité des réseaux et de l'information. CONTENU : en réponse à la demande du Conseil européen de Stockholm des 23 et 24 mars 2001, la présente communication de la Commission européenne formule une série de

recommandations visant à rendre l'Internet plus sûr pour les particuliers et les entreprises. La communication définit la sécurité des réseaux et de l'information, décrit les principales menaces qui pèsent sur la sécurité virus, piratage, refus de service, interception, mais également catastrophes naturelles et en conclut qu'une plus grande collaboration s'impose pour résoudre les problèmes. La Commission propose les mesures suivantes: - La sensibilisation est un élément essentiel: les utilisateurs doivent être en mesure d'apprécier parfaitement les risques liés à l'utilisation du réseau pour pouvoir choisir en connaissance de cause le niveau de sécurité qu'ils désirent. La Commission propose une mise en réseau plus efficace des systèmes européens de détection et d'information. - Pour certains problèmes de sécurité, il existe des solutions techniques, et il importe d'encourager une plus grande collaboration dans ce domaine. La Commission a intégré la problématique de la sécurité dans ses propositions relatives au 6e programme-cadre de R&D. - Pour être utiles, encore faut-il que les solutions soient interopérables. Les logiciels de chiffrement ne sont d'aucun secours si leur compatibilité n'est pas garantie de bout en bout. Il faut donc développer des standards communs et des solutions interopérables. - Les administrations publiques ont des responsabilités en ce qui concerne leurs propres systèmes. Les échanges de données à caractère médical, financier et personnel avec les administrations comptent parmi les plus sensibles. Si les administrations publiques montrent la voie à suivre en utilisant des solutions de sécurité interopérables pour leurs échanges électroniques, tant les particuliers que les entreprises seront amenés à prendre la sécurité des réseaux au sérieux. La Commission proposera dès lors de renforcer la coopération entre les équipes nationales d'intervention en cas d'urgence informatique (les CERT). - Le cadre juridique applicable en la matière doit tenir compte des nouveaux défis technologiques. À cet effet, la Commission dressera un inventaire des mesures nationales. Elle proposera également une mesure législative conformément au titre VI du traité sur l'Union européenne en matière d'attaques contre les systèmes informatiques, y compris le piratage et les attaques par refus de service. - Enfin, toute solution doit être replacée dans un contexte mondial. Le dialogue avec les partenaires internationaux de l'UE sera inscrit dans la stratégie de la Commission.

Communications électroniques: sécurité des réseaux et de l'information, rôle du secteur public

2001/2280(COS) - 22/10/2002 - Texte adopté du Parlement, lecture unique

En adoptant le rapport de Mme Ornella PACIOTTI (PSE, I), le Parlement européen estime que la sécurité des réseaux et de l'information n'est pas suffisamment assurée aujourd'hui et juge inadaptée une réponse fondée seulement sur une approche volontariste des acteurs en cause. Le Parlement souligne la nécessité de la formulation rapide de définitions communes de la sécurité et de l'intégrité des réseaux ainsi que de la sécurité de l'information. Il invite la Commission à élaborer un plan d'action pour l'encouragement de l'utilisation de la signature informatique, notamment grâce à l'adoption de normes européennes immédiatement opérationnelles au sein des institutions communautaires. Le Parlement réclame la définition d'une stratégie européenne qui, tout en restant neutre quant au type de technologie utilisée: - définisse ou actualise les normes applicables en matière de sécurité des réseaux de télécommunication et en assure l'interopérabilité; - favorise le développement de systèmes de codage et de certification à l'échelle européenne, et renforce les mesures destinées à protéger les données; - assure la prévention et la lutte efficace contre le crime dans le respect des garanties légales; - sensibilise les citoyens, les utilisateurs et les opérateurs publics et privés par des campagnes d'information au niveau national et européen favorisant la diffusion des meilleures pratiques en la matière. La Commission est également invitée à examiner en priorité les besoins en termes de sécurité et à procéder à des études sur un système de détection précoce dans le domaine des infrastructures électroniques pour les réseaux voués à la prestation: - d'infrastructures critiques, de services publics essentiels et de services tenant à la santé des personnes, - de systèmes de détection précoce et de leur interopérabilité, et - de services visant à encourager le développement du gouvernement en ligne et du commerce électronique. Le Parlement considère qu'une première intervention législative de l'Union dans ce contexte devrait se fonder sur les compétences qui lui sont reconnues en matière de réseaux transeuropéens (titre XV du traité CE) et, pour les aspects réclamant une harmonisation, en matière de marché intérieur (article 95 du traité CE). Il estime en outre que l'institution du groupe d'étude devrait être prévue par la même norme qui fixe les objectifs à poursuivre au niveau européen.