

Informations de base	
2017/2068(INI) INI - Procédure d'initiative	Procédure terminée
Lutte contre la cybercriminalité Subject 3.30.07 Cybersécurité, politique cyberspace 3.30.25 Réseaux mondiaux et société de l'information, internet 7.30.30 Lutte contre la criminalité	

Acteurs principaux			
Parlement européen	Commission au fond		Rapporteur(e)
	LIBE Libertés civiles, justice et affaires intérieures		VOZEMBERG-VRIONIDI Elissavet (PPE)
			Rapporteur(e) fictif/fictive DALLI Miriam (S&D) PROCTER John (ECR) GRIESBECK Nathalie (ALDE) ERNST Cornelia (GUE/NGL) ALBRECHT Jan Philipp (Verts/ALE)
	Commission pour avis		Rapporteur(e) pour avis
	INTA Commerce international		La commission a décidé de ne pas donner d'avis.
	ITRE Industrie, recherche et énergie		La commission a décidé de ne pas donner d'avis.
	IMCO Marché intérieur et protection des consommateurs		VAN BOSSUYT Anneleen (ECR)
			09/02/2017
	Formation du Conseil		Réunions
	Justice et affaires intérieures(JAI)		3539
Conseil de l'Union européenne			Date
			2017-05-18

Commission européenne	DG de la Commission	Commissaire
	Migration et affaires intérieures	AVRAMOPOULOS Dimitris

Événements clés			
Date	Événement	Référence	Résumé
18/05/2017	Adoption de résolution/conclusions par le Conseil		
18/05/2017	Annonce en plénière de la saisine de la commission		
11/07/2017	Vote en commission		
26/07/2017	Dépôt du rapport de la commission	A8-0272/2017	Résumé
02/10/2017	Débat en plénière		
03/10/2017	Décision du Parlement	T8-0366/2017	Résumé
03/10/2017	Résultat du vote au parlement		
03/10/2017	Fin de la procédure au Parlement		

Informations techniques	
Référence de la procédure	2017/2068(INI)
Type de procédure	INI - Procédure d'initiative
Sous-type de procédure	Rapport d'initiative
Base juridique	Règlement du Parlement EP 55
Autre base juridique	Règlement du Parlement EP 165
État de la procédure	Procédure terminée
Dossier de la commission	LIBE/8/09854

Portail de documentation				
Parlement Européen				
Type de document	Commission	Référence	Date	Résumé
Projet de rapport de la commission		PE604.566	11/05/2017	
Amendements déposés en commission		PE606.071	09/06/2017	
Amendements déposés en commission		PE606.072	09/06/2017	
Avis de la commission	IMCO	PE606.009	13/06/2017	
Rapport déposé de la commission, lecture unique		A8-0272/2017	26/07/2017	Résumé
Texte adopté du Parlement, lecture unique		T8-0366/2017	03/10/2017	Résumé
Commission Européenne				

Type de document	Référence	Date	Résumé
Réaction de la Commission sur le texte adopté en plénière	SP(2017)778	22/01/2018	

Lutte contre la cybercriminalité

2017/2068(INI) - 03/10/2017 - Texte adopté du Parlement, lecture unique

Le Parlement européen a adopté par 603 voix pour, 27 contre et 39 abstentions, une résolution sur la lutte contre la cybercriminalité.

Contexte: dans son évaluation de la menace que représente la criminalité organisée sur l'internet (IOCTA) du 28 septembre 2016, Europol indique que la cybercriminalité (rançongiciels, réseaux zombies, logiciels malveillants etc) **augmente en intensité, en complexité et en ampleur**. 80 % des entreprises en Europe ont connu au moins un incident de cybersécurité.

Les **enfants** sont particulièrement vulnérables face au risque d'être victimes du pédopiégeage et d'autres formes d'exploitation sexuelle en ligne. Un grand nombre d'actes de cybercriminalité ne font l'objet d'aucune poursuite et restent impunis.

Vu la nature transfrontalière de la cybercriminalité et les menaces communes en matière de cybersécurité auxquelles l'Union européenne est confrontée, le Parlement a demandé de **renforcer la coopération et l'échange d'informations** entre les autorités policières et judiciaires et les experts en cybercriminalité pour mener des enquêtes efficaces dans le cyberspace et obtenir des preuves électroniques.

Sur un plan général, les députés ont suggéré de **clarifier les définitions communes** de la cybercriminalité tout en soulignant que la lutte contre la cybercriminalité devrait viser avant tout **la protection et le renforcement des infrastructures critiques** dont, entre autres, les structures d'approvisionnement en énergie et en électricité et les structures financières. Ils ont condamné fermement toute atteinte à l'intégrité d'un système portée ou **dirigée par un pays étranger** ou par ses agents dans le but de perturber le processus démocratique d'un autre pays.

Le Parlement a également recommandé:

- d'adopter un **plan d'action** pour la protection des droits des enfants en ligne et hors ligne dans le cyberspace;
- de mettre en place toutes les mesures juridiques nécessaires pour lutter contre le phénomène de la violence en ligne à l'égard des femmes et le harcèlement en ligne;
- de donner à **Eurojust et à Europol** les moyens nécessaires pour améliorer l'identification des victimes, combattre les réseaux criminels d'agresseurs sexuels et accélérer la détection et le signalement de contenus pédopornographiques;
- de veiller à ce que les **contenus illicites** en ligne soient supprimés immédiatement par toutes voies de droit.

Prévention: dans le contexte de la révision de la stratégie de cybersécurité de l'Union européenne, la Commission est invitée à:

- **repérer les vulnérabilités en matière de sécurité des réseaux et de l'information dans les infrastructures critiques européennes**, à favoriser le développement de systèmes résilients et à évaluer la situation en ce qui concerne la lutte contre la cybercriminalité dans l'Union et les États membres;
- **lancer des campagnes de sensibilisation, d'information et de prévention** (assorties de programmes éducatifs) afin que les citoyens, en particulier les enfants, mais aussi les administrations, les opérateurs d'importance vitale et des acteurs du secteur privé, notamment les PME comprennent mieux les risques en matière de cybersécurité;
- promouvoir des mesures de sécurité telles que le **chiffrement** et des outils d'anonymisation.

Les États membres devraient **intensifier les échanges d'informations**, par l'intermédiaire d'Eurojust, d'Europol et de l'ENISA, ainsi que le partage des meilleures pratiques via le réseau européen des CSIRT (centres de réponse aux incidents de sécurité informatique) et des CERT (centres de réponse aux urgences informatiques). Ils devraient également **investir dans l'éducation** pour remédier à la pénurie de professionnels de l'informatique spécialisés dans la cybersécurité.

Renforcer la responsabilité des fournisseurs de services: les députés ont préconisé un renforcement de la coopération entre les autorités compétentes et les fournisseurs de services pour **accélérer l'entraide judiciaire**. Les fournisseurs de services de communications électroniques établis dans un **pays tiers** devraient désigner par écrit un représentant auprès de l'Union européenne.

Compte tenu de l'accessibilité croissante des dispositifs de **l'internet des objets**, les députés ont suggéré d'apporter une attention particulière à la sécurité de tous les dispositifs et de promouvoir l'option de la sécurité dès la conception. Ils ont souligné la nécessité de **protéger les bases de données des services répressifs** contre les incidents liés à la sécurité et l'accès illicite. Ils ont également encouragé les fournisseurs de services à adhérer au **code de conduite** visant à combattre les discours de haine illégaux en ligne.

Les États membres devraient créer des CERT auxquels les entreprises et les consommateurs pourraient **signaler les sites internet et les courriels malveillants**, comme le prévoit la **directive** sur la sécurité des réseaux d'information (SRI).

Renforcer la coopération policière et judiciaire: le Parlement a insisté sur la nécessité de permettre aux autorités répressives d'avoir **un accès licite aux informations pertinentes**, dans les cas restreints où cet accès est nécessaire pour des raisons de sécurité et de justice.

Les États membres **ne devraient pas imposer aux fournisseurs de services de chiffrement** d'obligations qui fragiliseraient la sécurité de leurs réseaux ou services, telles que la création ou la mise à disposition de «**portes dérobées**». Des solutions réalistes devraient être proposées lorsqu'il est indispensable de trouver de telles solutions pour des raisons de sécurité et de justice.

Selon les députés, **l'interception légale** pourrait être une mesure efficace pour combattre le piratage illicite, à condition qu'elle soit nécessaire, proportionnée, fondée sur une procédure judiciaire régulière et qu'elle respecte pleinement les droits fondamentaux.

Preuves électroniques: le Parlement a insisté sur la nécessité de trouver des moyens de recueillir des preuves électroniques plus rapidement et sur l'importance d'une **coopération étroite entre les autorités répressives, les pays tiers et les fournisseurs de services** actifs sur le territoire européen.

La Commission devrait proposer **un cadre juridique européen pour les preuves électroniques** comprenant des règles harmonisées pour déterminer le statut des fournisseurs de services, national ou étranger, et obliger ces derniers à répondre aux demandes en provenance d'autres États membres. Ce cadre devrait prévoir des garanties suffisantes concernant les droits et les libertés de toutes les parties concernées.

Enfin, le Parlement a déploré **l'absence d'une législation internationale contraignante** en matière de cybercriminalité et invité les États membres et les institutions européennes à œuvrer à l'élaboration d'une **convention** en la matière.

Lutte contre la cybercriminalité

2017/2068(INI) - 26/07/2017 - Rapport déposé de la commission, lecture unique

La commission des libertés civiles, de la justice et des affaires intérieures a adopté le rapport d'initiative d'Elissavet VOZEMBERG-VRIONIDI (PPE, EL) sur la lutte contre la cybercriminalité.

Contexte: l'évaluation de la menace que représente la criminalité organisée sur l'internet (IOCTA) du 28 septembre 2016, réalisée par Europol, indique que la cybercriminalité (rançongiciels, réseaux zombies, logiciels malveillants etc) **augmente en intensité, en complexité et en ampleur**, causant des dommages économiques et sociaux de plus en plus importants, ayant une incidence sur les droits fondamentaux des particuliers. 80% des entreprises en Europe ont connu au moins un incident de cybersécurité.

Les **enfants** qui utilisent l'internet de plus en plus tôt sont particulièrement vulnérables face au risque d'être victimes du pédopiéage et d'autres formes d'exploitation sexuelle en ligne.

Face à ces défis, le rapport suggère de **clarifier les définitions** de la cybercriminalité pour s'assurer que les institutions de l'Union et les États membres partagent des définitions juridiques communes.

Sur un plan général, les députés recommandent de:

- transposer rapidement la [directive 2011/93/UE](#) relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et d'adopter un **plan d'action** pour la protection des droits des enfants en ligne et hors ligne dans le cyberspace;
- mettre en place toutes les mesures juridiques nécessaires pour lutter contre le phénomène de la violence en ligne à l'égard des femmes et le harcèlement en ligne;
- veiller à ce que les **contenus illicites en ligne** soient supprimés immédiatement par toutes voies de droit.

Pour être efficaces, les stratégies de cybersécurité devraient être fondées sur les libertés et les droits fondamentaux.

Prévention: dans le contexte de la révision de la stratégie de cybersécurité de l'Union européenne, la Commission est invitée à:

- **repérer les vulnérabilités en matière de sécurité des réseaux et de l'information dans les infrastructures critiques européennes**, à favoriser le développement de systèmes résilients et à évaluer la situation en ce qui concerne la lutte contre la cybercriminalité dans l'Union et les États membres;
- **lancer des campagnes de sensibilisation, d'information et de prévention** (assorties de programmes éducatifs), afin de veiller à ce que tous les citoyens, en particulier les enfants et les autres utilisateurs vulnérables, mais aussi les administrations centrales et locales, les opérateurs d'importance vitale et les acteurs du secteur privé, notamment les PME, aient conscience des risques posés par la cybercriminalité.

Les États membres devraient **intensifier les échanges d'informations**, par l'intermédiaire d'Eurojust, d'Europol et de l'ENISA, ainsi que le partage des meilleures pratiques via le réseau européen des CSIRT (centres de réponse aux incidents de sécurité informatique) et des CERT (centres de réponse aux urgences informatiques), en ce qui concerne les problèmes auxquels ils sont confrontés dans la lutte contre la cybercriminalité.

Renforcer la responsabilité des fournisseurs de services: les députés préconisent un renforcement de la coopération entre les autorités compétentes et les fournisseurs de services pour **accélérer l'entraide judiciaire** et les procédures de reconnaissance mutuelle, dans les domaines de compétence prévus dans le cadre juridique européen. Les fournisseurs de services de communications électroniques établis dans un pays tiers devraient désigner par écrit un représentant auprès de l'Union européenne.

Compte tenu des tendances de l'innovation et de l'accessibilité croissante des dispositifs de l'internet des objets, les députés suggèrent d'apporter une attention particulière à la sécurité de tous les dispositifs et de promouvoir l'option de la sécurité dès la conception. Ils soulignent la nécessité de **protéger les bases de données des services répressifs** contre les incidents liés à la sécurité et l'accès illicite. Ils encouragent également les fournisseurs de services à adhérer au **code de conduite** visant à combattre les discours de haine illégaux en ligne.

Renforcer la coopération policière et judiciaire: le rapport insiste sur la nécessité de permettre aux autorités répressives d'avoir **un accès licite aux informations pertinentes**, dans les cas restreints où cet accès est nécessaire et proportionné pour des raisons de sécurité et de justice.

Les députés invitent les États membres à **ne pas imposer aux fournisseurs de services de chiffrement** d'obligations qui fragiliseraient la sécurité de leurs réseaux ou services, telles que la création ou la mise à disposition de «**portes dérobées**». Des solutions réalistes devraient être proposées lorsqu'il est indispensable de trouver de telles solutions pour des raisons de sécurité et de justice.

Selon les députés, l'interception légale pourrait être une mesure efficace pour combattre le piratage illicite, à condition qu'elle soit nécessaire, proportionnée, fondée sur une procédure judiciaire régulière et qu'elle respecte pleinement les droits fondamentaux.

Preuves électroniques: le rapport plaide pour une **approche européenne** commune en matière de justice pénale. Il insiste sur la nécessité de trouver des moyens de recueillir des preuves électroniques plus rapidement et sur l'importance d'une **coopération étroite entre les autorités répressives, les pays tiers et les fournisseurs de services** actifs sur le territoire européen.

En vue de **renforcer les capacités au niveau européen**, le rapport invite l'ENISA à évaluer de façon continue le niveau de menace. Il encourage la Commission à investir dans les capacités informatiques ainsi que dans la défense des infrastructures critiques des institutions de l'Union afin de réduire la vulnérabilité de l'Union face à de graves attaques informatiques provenant d'organisations criminelles d'envergure.