Procedure file

Informations de base

INI - Procédure d'initiative	2017/2068(INI)	Procédure terminée
Lutte contre la cybercriminalité Sujet 3.30.07 Cybersécurité, politique cyberespace 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)	Date de nomination
	LIBE Libertés civiles, justice et affaires intérieures		30/01/2017
		VOZEMBERG-VRIONIDI Elissavet	
		Rapporteur(e) fictif/fictive	
		DALLI Miriam	
		PROCTER John	
		GRIESBECK Nathalie	
		ALBRECHT Jan Philipp	
	Commission pour avis	Rapporteur(e) pour avis	Date de nomination
	ITRE Industrie, recherche et énergie	La commission a décidé de ne pas donner d'avis.	
	IMCO Marché intérieur et protection des consommateurs		09/02/2017
		VAN BOSSUYT Anneleen	
	INTA Commerce international	La commission a décidé de ne pas donner d'avis.	
Conseil de l'Union européenne	Formation du Conseil	Réunion	Date
	Justice et affaires intérieures(JAI)	3539	18/05/2017
Commission européenne	DG de la Commission	Commissaire	
	Migration et affaires intérieures	AVRAMOPOULOS Dimitris	

Evénements clés

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	Résultat du vote au parlement		
03/10/2017	Décision du Parlement	T8-0366/2017	Résumé
03/10/2017	Fin de la procédure au Parlement		

Informations techniques

Référence de procédure	2017/2068(INI)
Type de procédure	INI - Procédure d'initiative
Sous-type de procédure	Rapport d?initiative
Base juridique	Règlement du Parlement EP 54
Autre base juridique	Règlement du Parlement EP 159
Etape de la procédure	Procédure terminée
Dossier de la commission parlementaire	LIBE/8/09854

Portail de documentation

Projet de rapport de la commission		PE604.566	11/05/2017	EP	
Amendements déposés en commission		PE606.071	09/06/2017	EP	
Amendements déposés en commission		PE606.072	09/06/2017	EP	
Avis de la commission	IMCO	PE606.009	13/06/2017	EP	
Rapport déposé de la commission, lecture unique		A8-0272/2017	26/07/2017	EP	Résumé
Texte adopté du Parlement, lecture unique		T8-0366/2017	03/10/2017	EP	Résumé
Réaction de la Commission sur le texte adopté en plénière		SP(2017)778	22/01/2018	EC	

Lutte contre la cybercriminalité

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

Contexte: lévaluation de la menace que représente la criminalité organisée sur linternet (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 linternet de plus en plus tôt sont particulièrement vulnérables face au risque dêtre victimes du pédopiégeage et dautres formes dexploitation sexuelle en ligne.

Face à ces défis, le rapport suggère de clarifier les définitions de la cybercriminalité pour sassurer que les institutions de lUnion 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 lexploitation sexuelle des enfants, ainsi que la pédopornographie et dadopter un plan daction pour la protection des droits des enfants en ligne et hors ligne dans le cyberespace;
- mettre en place toutes les mesures juridiques nécessaires pour lutter contre le phénomène de la violence en ligne à légard 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 lUnion européenne, la Commission est invitée à:

- repérer les vulnérabilités en matière de sécurité des réseaux et de linformation 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 lUnion et les États membres;
- lancer des campagnes de sensibilisation, dinformation 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 dimportance 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 dinformations, par lintermédiaire dEurojust, dEuropol et de lENISA, 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 lentraide 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 lUnion européenne.

Compte tenu des tendances de linnovation et de laccessibilité croissante des dispositifs de linternet des objets, les députés suggèrent dapporter une attention particulière à la sécurité de tous les dispositifs et de promouvoir loption 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 laccès 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 davoir 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 dobligations 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 lorsquil est indispensable de trouver de telles solutions pour des raisons de sécurité et de justice.

Selon les députés, linterception légale pourrait être une mesure efficace pour combattre le piratage illicite, à condition quelle soit nécessaire, proportionnée, fondée sur une procédure judiciaire régulière et quelle 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 limportance dune 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 lENISA 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 lUnion afin de réduire la vulnérabilité de lUnion face à de graves attaques informatiques provenant dorganisations criminelles denvergure.

Lutte contre la cybercriminalité

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 linternet (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 dêtre victimes du pédopiégeage et dautres formes dexploitation sexuelle en ligne. Un grand nombre dactes de cybercriminalité ne font lobjet daucune poursuite et restent impunis.

Vu la nature transfrontalière de la cybercriminalité et les menaces communes en matière de cybersécurité auxquelles lUnion européenne est confrontée, le Parlement a demandé de renforcer la coopération et léchange dinformations entre les autorités policières et judiciaires et les experts en cybercriminalité pour mener des enquêtes efficaces dans le cyberespace 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 dapprovisionnement en énergie et en électricité et les structures financières. Ils ont condamné fermement toute atteinte à lintégrité dun système portée ou dirigée par un pays étranger ou par ses agents dans le but de perturber le processus démocratique dun autre pays.

Le Parlement a également recommandé:

- dadopter un plan daction pour la protection des droits des enfants en ligne et hors ligne dans le cyberespace;
- de mettre en place toutes les mesures juridiques nécessaires pour lutter contre le phénomène de la violence en ligne à légard des femmes et le harcèlement en ligne;
- de donner à Eurojust et à Europol les moyens nécessaires pour améliorer lidentification des victimes, combattre les réseaux criminels dagresseurs 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 lUnion européenne, la Commission est invitée à:

- repérer les vulnérabilités en matière de sécurité des réseaux et de linformation 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 lUnion et les États membres;

- lancer des campagnes de sensibilisation, dinformation et de prévention (assorties de programmes éducatifs) afin que les citoyens, en particulier les enfants, mais aussi les administrations, les opérateurs dimportance 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 danonymisation.

Les États membres devraient intensifier les échanges dinformations, par lintermédiaire dEurojust, dEuropol et de lENISA, 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 léducation pour remédier à la pénurie de professionnels de linformatique 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 lentraide judiciaire. Les fournisseurs de services de communications électroniques établis dans un pays tiers devraient désigner par écrit un représentant auprès de lUnion européenne.

Compte tenu de laccessibilité croissante des dispositifs de linternet des objets, les députés ont suggéré dapporter une attention particulière à la sécurité de tous les dispositifs et de promouvoir loption 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 laccès 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 dinformation (SRI).

Renforcer la coopération policière et judiciaire: le Parlement a insisté sur la nécessité de permettre aux autorités répressives davoir 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 dobligations 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 lorsquil est indispensable de trouver de telles solutions pour des raisons de sécurité et de justice.

Selon les députés, linterception légale pourrait être une mesure efficace pour combattre le piratage illicite, à condition quelle soit nécessaire, proportionnée, fondée sur une procédure judiciaire régulière et quelle 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 limportance dune 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 dautres 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 labsence dune législation internationale contraignante en matière de cybercriminalité et invité les États membres et les institutions européennes à uvrer à lélaboration dune convention en la matière.