Parlement européen
2014-2019

Commission des libertés civiles, de la justice et des affaires intérieures

2017/2068(INI)

.5.2017

PROJET DE RAPPORT

sur la lutte contre la cybercriminalité
(2017/2068(INI))

Commission des libertés civiles, de la justice et des affaires intérieures

Rapporteure: Elissavet Vozemberg-Vrionidi

PR_INI

SOMMAIRE

Page

PROPOSITION DE RÉSOLUTION DU PARLEMENT EUROPÉEN

sur la lutte contre la cybercriminalité
(2017/2068(INI))

Le Parlement européen,

– vu les articles 2, 3 et 6 du traité sur l'Union européenne (traité UE),

– vu les articles 16, 67, 70, 72, 73, 75, 82, 83, 84, 87 et 88 du traité sur le fonctionnement de l'Union européenne (traité FUE),

– vu les articles 1, 7, 8, 11, 21, 24 et 52 de la Charte des droits fondamentaux de l'Union européenne,

– vu la décision-cadre du Conseil du 28 mai 2001 concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces[1],

– vu la convention de Budapest sur la cybercriminalité du 23 novembre 2001[2],

– vu le règlement (CE) nº 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information[3],

– vu la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection[4],

– vu la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques[5],

– vu la directive 2011/92/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil[6],

– vu la communication conjointe du 7 février 2013 au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, de la Commission européenne et de la vice-présidente de la Commission/haute représentante de l'Union pour les affaires étrangères et la politique de sécurité, intitulée «Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé» (JOIN(2013)0001),

– vu la directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013

[1] JO L 149 du 2.6.2001, p. 1.
[2] Conseil de l'Europe, Série des traités européens nº 185, 23.11.2001.
[3] JO L 77 du 13.3.2004, p. 1.
[4] JO L 345 du 23.12.2008, p. 75.
[5] JO L 201 du 31.7.2002, p. 37.
[6] JO L 335 du 17.12.2011, p. 1.

relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil[1],

– vu la directive 2014/41/UE du Parlement européen et du Conseil du 3 avril 2014 concernant la décision d'enquête européenne en matière pénale[2],

– vu sa résolution du 12 septembre 2013 sur la stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé[3],

– vu la communication de la Commission du mardi 28 avril 2015, intitulée «Stratégie pour un marché unique numérique en Europe» (COM(2015)0192),

– vu la communication de la Commission du 28 avril 2015 intitulée «Le programme européen en matière de sécurité» (COM(2015)0185) et les rapports de suivi intitulés «Vers une union de la sécurité réelle et effective»,

– vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données - PIBR)[4],

– vu la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil[5],

– vu le règlement (UE) 2016/794 du Parlement européen et du Conseil du 11 mai 2016 relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol)[6],

– vu la décision de la Commission du 5 juillet 2016 relative à la signature d'un accord contractuel concernant un partenariat public-privé pour la recherche et l'innovation industrielles dans le domaine de la cybersécurité entre l'Union européenne, représentée par la Commission, et l'organisation partenaire (C(2016)4400),

– vu la communication conjointe au Parlement européen et au Conseil du 6 avril 2016 intitulée: «Cadre commun en matière de lutte contre les menaces hybrides: une réponse de l'Union européenne» (JOIN(2016)0018),

– vu la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant les mesures destinées à assurer un niveau élevé commun de sécurité des

[1] JO L 218 du 14.8.2013, p.8.
[2] JO L 130 du 1.5.2014, p. 1.
[3] JO C 93 du 9.3.2016, p. 112.
[4] JO L 119 du 4.5.2016, p. 1.
[5] JO L 119 du 4.5.2016, p. 89.
[6] JO L 135 du 24.5.2016, p. 53

réseaux et des systèmes d'information dans l'Union[1],

– vu le rapport final du groupe sur les preuves dans le nuage (*Cloud Evidence Group*) T-CY du Conseil de l'Europe sur la cybercriminalité intitulé «Accès de la justice pénale aux preuves électroniques dans le cloud : Recommandations pour examen par le T-CY» du 16 septembre 2016,

– vu l'évaluation de la menace que représente la grande criminalité organisée (SOCTA) du 28 février 2017 et l'évaluation de la menace que représente la criminalité organisée sur l'internet (IOCTA) du 28 septembre 2016, réalisées par Europol,

– vu l'arrêt de la Cour de justice de l'Union européenne dans l'affaire C-203/15 (arrêt TELE2) du 21 décembre 2016[2],

– vu la directive (UE) 2017/541/UE du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil[3],

– vu l'article 52 de son règlement,

– vu le rapport de la commission des libertés civiles, de la justice et des affaires intérieures (A8-0000/2017),

A. considérant que la cybercriminalité cause des dommages économiques et sociaux de plus en plus importants, ayant une incidence sur les droits fondamentaux des particuliers, posant une menace à l'encontre de l'État de droit dans le cyberespace et mettant en danger la stabilité de nos sociétés démocratiques;

B. considérant que les lignes entre la cybercriminalité, le cyberespionnage, la guerre informatique, le cyber-sabotage et le cyberterrorisme sont de plus en plus floues; que la cybercriminalité peut cibler des individus, des entités publiques ou bien privées et couvrir un large éventail d'infractions, y compris les atteintes à la vie privée, la violation des droits d'auteur en ligne, la pédopornographie, l'incitation en ligne à la haine, la diffusion de fausses informations avec intention malveillante, la criminalité financière et la fraude, ainsi que l'atteinte illégale à l'intégrité de systèmes;

C. considérant que l'évaluation de la menace que représente la criminalité organisée sur l'internet (IOCTA) de 2016 indique que la cybercriminalité augmente en intensité, en complexité et en ampleur, que la cybercriminalité déclarée dépasse la criminalité traditionnelle dans certains pays de l'Union européenne, qu'elle s'étend à d'autres domaines de la criminalité, tels que la traite des êtres humains, qu'il y a eu un abus croissant des outils de cryptage et d'anonymisation et que les attaques à l'aide de rançongiciels sont plus nombreuses que les logiciels malveillants tels que des chevaux de Troie;

---

[1] JO L 194 du 19.7.2016, p. 1.
[2] Arrêt de la Cour de justice de l'Union européenne du 21 décembre 2016, *Tele2 Sverige AB* contre *Post- och telestyrelsen* et *Secretary of State for the Home Department* contre *Tom Watson e.a.*, C-203/15, ECLI:EU:C:2016:970.
[3] JO L 88 du 31.3.2017, p. 6.

D. considérant que la cible principale des attaques informatiques demeure les données personnelles sensibles telles que les documents de santé ou les documents financiers, mais que les attaques sur les systèmes et les réseaux de contrôle industriel visant à détruire les structures économiques et à déstabiliser les sociétés vont croissantes; que la majorité des demandes internationales de données sont relatives à la fraude et la criminalité financière, suivies des formes violentes et graves de criminalité;

E. considérant qu'un nombre considérable d'actes de cybercriminalité demeurent impunis et font l'objet d'une impunité, en partie en raison d'une sous-déclaration importante, de longues périodes de détection permettant aux cybercriminels de développer des entrées/sorties multiples ou des portes dérobées, d'un accès peu aisé aux preuves électroniques, des difficultés à se les procurer et à faire valoir leur recevabilité en justice, ainsi que de la complexité des procédures et des problèmes de compétence liés à la nature transfrontalière de la cybercriminalité;

F. considérant que l'arrêt TELE2 de la CJUE impose des limites strictes à l'accès, par la police et l'appareil judiciaire, aux données des personnes soupçonnées d'actes de cybercriminalité;

G. considérant que les enfants sont particulièrement vulnérables aux sollicitations en ligne à des fins sexuelles et aux autres formes d'exploitation sexuelle en ligne, et nécessitent donc une protection spéciale;

H. considérant que la sensibilisation aux risques posés par la cybercriminalité a augmenté, mais que des mesures conservatoires, tant de la part des utilisateurs individuels que des entreprises, se font toujours attendre;

I. considérant que l'interconnexion des personnes, des lieux et des choses, laquelle ne cesse de croître, fait des dispositifs de l'internet des objets (IdO) une cible idéale pour les cybercriminels;

Considérations générales

1. souligne que la forte augmentation des rançongiciels, des réseaux zombies et de toute déficience des systèmes informatiques a une incidence sur la disponibilité et l'intégrité des données à caractère personnel, ainsi que sur la protection de la vie privée et des libertés fondamentales;

2. rappelle l'importance des mesures juridiques prises au niveau européen afin d'harmoniser la définition des infractions liées aux attaques contre les systèmes d'information ainsi qu'à l'exploitation sexuelle des enfants en ligne, et d'obliger les États membres à mettre en place un système d'enregistrement, de production et de communication de statistiques sur ces infractions;

3. déplore que les attaques informatiques à l'encontre d'entreprises passent souvent inaperçues ou ne soient pas déclarées; estime que l'obligation de dévoiler les atteintes à la sécurité instaurée par le PIBR permettra de remédier à ce problème;

4. souligne que le phénomène de l'évolution constante du paysage des cyber-menaces pose pour toutes les parties prenantes de graves problèmes juridiques et technologiques;

insiste, en particulier, sur la recrudescence de l'utilisation abusive des technologies de protection de la vie privée telles que le routage en oignon et le Darknet, ainsi que sur les menaces croissantes que posent les pirates informatiques parrainées par des pays étrangers non-amis ou des organisations politiques ou religieuses extrémistes;

5. constate que le recours, par les extrémistes, à des outils et des services de cybercriminalité demeure limité; souligne, toutefois, que cette situation pourrait changer à la lumière des liens de plus en plus étroits entre terrorisme et criminalité organisée, ainsi que de la disponibilité d'armes à feu et de précurseurs d'explosifs sur le Darknet;

6. constate que les avancées technologiques en matière de cryptage permettent aux utilisateurs légitimes de mieux protéger leurs données, mais souligne que les utilisateurs malintentionnés déploient les mêmes techniques pour dissimuler leurs activités criminelles et leur identité;

7. invite les États membres à redoubler d'efforts en ce qui concerne l'identification des victimes et les services d'aide aux victimes;

Prévention

8. invite la Commission, dans le contexte de la révision de la stratégie de cybersécurité de l'Union européenne, à évaluer la situation en ce qui concerne la lutte contre la cybercriminalité dans l'Union européenne et les États membres, afin de parvenir à une meilleure compréhension des tendances et de l'évolution de la situation en ce qui concerne les infractions dans le cyberespace;

9. souligne que la cyber-résilience est essentielle dans la prévention de la cybercriminalité et devrait donc se voir accorder la plus haute priorité; appelle de ses vœux une approche européenne globale en matière de lutte contre la cybercriminalité qui soit compatible avec les droits fondamentaux, la protection des données, la cybersécurité, la protection des consommateurs et le commerce électronique;

10. salue, à cet égard, l'investissement de fonds de l'Union dans des projets de recherche tels que le partenariat public-privé (PPP) sur la cybersécurité, afin de favoriser la cyber-résilience grâce à l'innovation et au renforcement des capacités;

11. invite instamment les États membres à intensifier les échanges d'informations sur les problèmes auxquels ils sont confrontés dans le domaine de la lutte contre la cybercriminalité, ainsi que sur les solutions envisageables pour y remédier;

12. est préoccupé par le fait qu'Europol a constaté que la majorité des attaques menées avec succès sont imputables à une sensibilisation insuffisante des utilisateurs, ainsi qu'à une sécurité insuffisante;

13. invite la Commission et les États membres à lancer des campagnes de sensibilisation afin de garantir que tous les citoyens, et en particulier les enfants et les autres usagers vulnérables, et le secteur privé prennent conscience des risques posés par la cybercriminalité, et à promouvoir le recours à des mesures de sécurité telles que le cryptage;

14. souligne que les entreprises devraient mener régulièrement des évaluations de la vulnérabilité, remédier aux vulnérabilités existantes dans leurs produits ou services et signaler systématiquement les cyberattaques;

15. prie instamment les États membres d'investir dans une meilleure sécurisation de leurs infrastructures critiques et données connexes afin de faire face aux cyberattaques;

Renforcement de la responsabilité et de la responsabilité des prestataires de services

16. estime que le renforcement de la coopération avec les prestataires de services doit être un facteur clé pour accélérer et rationaliser l'entraide judiciaire et les procédures de reconnaissance mutuelle;

17. estime que l'innovation ne devrait pas être entravée par des lourdeurs administratives inutiles pour les développeurs de logiciels et les producteurs; encourage le secteur privé à mettre en œuvre des mesures volontaires visant à renforcer la confiance dans la sécurité des logiciels et dispositifs, tels que le label de confiance de l'internet des objets;

18. invite la Commission à présenter des mesures législatives établissant des définitions claires et des sanctions minimales pour la diffusion de fausses informations en ligne et l'incitation à la haine, les obligations incombant aux fournisseurs de services Internet ainsi que des sanctions en cas de non-respect;

19. invite la Commission à enquêter sur les possibilités juridiques d'amélioration de la responsabilité des prestataires de services et d'imposition d'une obligation de répondre aux demandes adressées de l'étranger à des services répressifs dans l'Union;

20. invite les États membres à imposer les mêmes obligations de cryptage aux prestataires de services en ligne que celles qui s'appliquent aux prestataires de services de télécommunications traditionnels;

21. souligne que les contenus illicites en ligne doivent être immédiatement supprimés; se félicite, dans ce contexte, de l'état d'avancement des travaux concernant le blocage et la suppression des contenus illicites en ligne, mais insiste sur la nécessité d'un engagement plus fort de la part des prestataires de services des plateformes à répondre rapidement et efficacement;

Renforcer la coopération policière et judiciaire

22. est préoccupé par le fait qu'un nombre considérable d'actes de cybercriminalité demeurent impunis; insiste sur la nécessité de permettre un accès licite aux informations pertinentes, même si elles ont été cryptées, si cet accès est indispensable pour des raisons de sécurité et de justice;

23. invite instamment les États membres à échanger les pratiques éprouvées en ce qui concerne le contournement du cryptage et à coopérer, en consultation avec le pouvoir judiciaire, dans l'harmonisation des conditions de l'utilisation licite des outils d'investigation en ligne;

24. souligne que le piratage légal doit être une mesure de dernier recours, qui doit être

nécessaire, proportionnée et pleinement respectueuse des droits fondamentaux et de la protection des données dans l'Union ainsi que de la jurisprudence; invite tous les États membres à établir des règles claires en ce qui concerne la procédure d'autorisation des activités de piratage légal, y compris les restrictions sur l'utilisation et la durée des outils de piratage légal, à mettre en place un mécanisme de surveillance, et à prévoir les voies de droit efficaces pour les victimes de ces activités de piratage;

25. invite les États membres à s'informer mutuellement en cas de violation de leur souveraineté territoriale dans le cadre des enquêtes menées en raison du manque d'informations concernant la localisation du dispositif de piratage;

26. insiste sur la nécessité de réduire au maximum les risques que posent, pour la vie privée des utilisateurs de l'internet, les fuites des exploits ou des outils utilisés par les services répressifs dans le cadre de leurs enquêtes légitimes;

27. souligne que les autorités judiciaires et répressives doivent être dotées de capacités et de ressources suffisantes afin de répondre de manière efficace à la lutte contre la cybercriminalité;

28. souligne que la multitude de juridictions nationales distinctes et définies territorialement crée des difficultés dans la détermination de la loi applicable dans des interactions transnationales et donne lieu à une insécurité juridique, empêchant ainsi la coopération par-delà les frontières, laquelle est nécessaire pour traiter efficacement les abus en ligne;

Preuves électroniques

29. souligne qu'une approche européenne commune à l'égard de la justice pénale dans le cyberespace constitue une priorité, car elle contribuera à améliorer le respect de l'état de droit dans le cyberespace et facilitera l'obtention de preuves électroniques dans le cadre de procédures pénales;

30. souligne l'importance d'une coopération étroite entre les services répressifs et le secteur privé sur la question de l'accès aux preuves numériques; invite instamment les États membres concernés à éliminer les dispositions de droit pénal interdisant aux prestataires nationaux de répondre aux demandes de services répressifs étrangers;

31. invite la Commission à proposer un cadre juridique européen pour les preuves électroniques comprenant des règles harmonisées pour déterminer le statut de prestataires de services, qu'ils soient nationaux ou étrangers, et obliger ces derniers à répondre aux demandes en provenance de pays tiers, afin de garantir une sécurité juridique pour les parties prenantes et de supprimer les obstacles à la coopération;

32. invite les États membres à mettre pleinement en œuvre la directive concernant la décision d'enquête européenne en matière pénale aux fins de recueillir et d'obtenir efficacement des preuves électroniques dans l'Union, ainsi qu'à prévoir des dispositions spécifiques relatives au cyberespace dans leurs codes pénaux nationaux afin de contribuer à la recevabilité des preuves électroniques devant les tribunaux et à émettre des orientations plus claires à l'intention des juges en ce qui concerne la pénalisation de la cybercriminalité;

Renforcement des capacités au niveau européen

33. constate la contribution importante qu'apportent les agences de la justice et des affaires intérieures (JAI), en particulier le Centre européen de lutte contre la cybercriminalité (EC3) Europol et Eurojust, ainsi que l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA), à la lutte contre la cybercriminalité;

34. invite Europol à soutenir les autorités répressives nationales dans la mise en place de voie de transmission sûres et adéquates;

35. demande à l'Agence de l'Union européenne pour la formation des services répressifs (CEPOL) et au Réseau européen de formation judiciaire d'étendre leur offre de formations consacrées à des thèmes touchant à la cybercriminalité aux instances chargées de faire respecter la loi et aux autorités judiciaires à travers l'Union;

36. appelle de ses vœux un financement suffisant et la mise à disposition de postes de l'Unité de coopération judiciaire de l'Union européenne (Eurojust) afin de permettre à l'agence de faire face à sa charge de travail croissante, ainsi que de développer et de renforcer son soutien aux procureurs spécialisés dans la cybercriminalité dans les cas transfrontaliers, notamment par l'intermédiaire du réseau judiciaire européen en matière de cybercriminalité, récemment créé;

Amélioration de la coopération avec les pays tiers

37. insiste sur l'importance d'une coopération étroite avec les pays tiers dans le cadre de la lutte contre la cybercriminalité, y compris au moyen de l'échange des pratiques éprouvées, d'enquêtes communes, du renforcement des capacités et de l'assistance juridique mutuelle;

38. souligne que les accords de coopération stratégique et opérationnelle entre Europol et les pays tiers facilitent les échanges d'informations et la coopération pratique; invite Europol à conclure des accords avec tous les pays énumérés dans l'annexe du règlement Europol en temps utile;

39. prend acte du fait que le plus grand nombre de demandes émanant des services répressifs sont transmises aux États-Unis et au Canada; est préoccupé par le fait que le taux de divulgation volontaire des grands prestataires américains en réponse aux demandes formulées par les autorités de justice pénale européennes soit bien en deçà des 60 %;

40. invite la Commission à présenter des mesures concrètes pour remédier aux obstacles à l'échange d'informations entre les services répressifs européens et les pays tiers, notamment en ce qui concerne l'obtention rapide, sur la base d'une décision judiciaire, d'éléments de preuve pertinents, des données des abonnés ainsi que des métadonnées et des données relatives au contenu (si elles ne sont pas cryptées) de services répressifs et/ou de prestataires de services en vue d'améliorer l'entraide judiciaire;

41. soutient l'aide au renforcement des capacités fournie par l'Union européenne aux pays du voisinage oriental, étant donné que de nombreuses cyberattaques y trouvent leur origine;

°

° °

42. charge son Président de transmettre la présente résolution au Conseil et à la Commission.