# 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 pédopiégeage 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 cyberespace;
- 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.