

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 pédopiéage 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.