Coopération judiciaire pénale: lutte contre attaques visant les systèmes d'information

2010/0273(COD) - 09/06/2011

Le Conseil a adopté une **orientation générale** concernant un projet de directive relative aux attaques visant les systèmes d'information, proposé par la Commission en septembre 2010. Cette orientation générale servira de base au Conseil lors des négociations avec le Parlement européen sur cette proposition dans le cadre de la procédure législative ordinaire.

La proposition a pour objet de mettre à jour les règles existantes, qui datent de 2005 (décision cadre 2005 /222/JAI), tout en s'appuyant sur la convention du Conseil de l'Europe sur la cybercriminalité (convention de Budapest). La nouvelle réglementation reprendrait la plupart des dispositions en place - à savoir la pénalisation de l'accès illicite, l'atteinte à l'intégrité d'un système, l'atteinte à l'intégrité des données, ainsi que l'instigation, la complicité et la tentative d'infraction - et **comprend les nouveaux éléments suivants**:

- la pénalisation de la production et de la mise à disposition d'outils (par exemple, des logiciels malveillants conçus pour créer des «zombies», ou des mots de passe obtenus de manière frauduleuse) en vue de commettre des infractions;
- l'interception illégale de données informatiques devient une infraction;
- l'amélioration de la coopération en matière pénale en Europe en consolidant la structure existante des points de contact opérationnels 24h/24, 7 jours/7, y compris l'obligation d'assurer un retour d'information dans un délai de 8 heures en cas de demande urgente; et
- l'obligation de collecter les données statistiques de base sur la cybercriminalité.

En ce qui concerne le niveau des **sanctions pénales**, la nouvelle réglementation **relèverait les seuils**:

- en règle générale, à une peine d'emprisonnement maximale d'au moins deux ans;
- si l'infraction commise affecte un nombre significatif de systèmes informatiques, par exemple pour créer des "zombies", à une peine d'emprisonnement maximale d'au moins trois ans;
- si l'attaque a été commise par un groupe criminel organisé, qu'elle a causé un grave préjudice, par exemple par l'utilisation de "zombies", ou qu'elle a touché un système informatique critique, à une peine d'emprisonnement maximale d'au moins cinq ans.

Ces nouvelles formes de circonstances aggravantes ont pour but de faire face aux nouvelles menaces que représentent les cyberattaques à grande échelle, dont le nombre ne cesse d'augmenter en Europe et qui sont susceptibles de menacer gravement les intérêts publics.

Enfin, le Conseil a précisé les règles relatives à l'établissement d'une compétence juridictionnelle des États membres en matière de cybercriminalité.

Le Royaume-Uni et l'Irlande participent à l'adoption et à l'application de cette directive, qui ne liera par contre pas le Danemark.