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

2010/0273(COD) - 30/09/2010 - Document de base législatif

OBJECTIF: proposer un nouveau cadre législatif destiné à lutter contre les attaques (notamment les attaques de grande ampleur) visant les systèmes d'information et abroger la décision-cadre 2005/222/JAI du Conseil.

ACTE PROPOSÉ : Directive du Parlement européen et du Conseil.

CONTEXTE : la cybercriminalité souffre de la grande divergence des législations et procédures pénales nationales pour lutter contre ce phénomène, si bien que le traitement réservé à ces infractions n'est pas uniforme. L'insuffisance des mesures prises dans le cadre des mécanismes répressifs pour lutter contre la cybercriminalité contribue par ailleurs à sa prévalence, certains types d'infractions ayant un caractère transnational. L'évolution des technologies de l'information aggrave encore le problème en facilitant la production et la distribution d'outils («maliciels» et «botnets») offrant l'anonymat aux délinquants et éparpillant la responsabilité entre divers pays. La difficulté d'engager des poursuites qui en résulte permet ainsi à la criminalité organisée de réaliser des profits considérables à peu de risques.

La décision-cadre 2005/222/JAI du Conseil relative aux attaques visant les systèmes d'information visait à renforcer la coopération entre les autorités judiciaires et les autres autorités compétentes, notamment la police et les autres services spécialisés chargés de l'application de la loi dans les États membres, grâce à un rapprochement de leurs règles pénales réprimant les attaques contre les systèmes d'information. Les États membres étaient tenus de transposer ce texte pour le 16 mars 2007 au plus tard. Toutefois, le rapport de mise en œuvre de cette décision-cadre a montré que ce texte ne permettait pas de contrer des attaques massives commises simultanément contre plusieurs systèmes d'information comme l'utilisation accrue des "botnets" ou «réseaux zombies» à des fins criminelles.

Pour faire face à ces évolutions, la Commission propose maintenant de refondre la décision-cadre de 2005 pour prévoir un cadre législatif rénové permettant de répondre à des menaces de grande ampleur, comme les attaques de «botnets» ou de «réseaux zombies» particulièrement dévastatrices (un «réseau zombies» est constitué d'un groupe d'ordinateurs contaminés par des virus informatiques dormants à l'insu de leurs utilisateurs et pouvant être activé à distance pour exécuter certaines actions parfois de grande ampleur, comme l'attaque de systèmes d'information ou des cyber-attaques).

ANALYSE D'IMPACT : diverses options d'action ont été étudiées :

- ***Option 1*** - Statu quo/pas de nouvelle action de l'Union.
- ***Option 2*** - élaboration d'un programme intensifiant les efforts de lutte contre les attaques visant les systèmes d'information par des mesures non législatives : ces instruments non contraignants encourageraient une action plus coordonnée au niveau de l'Union, notamment la consolidation de l'actuel réseau 24/7 de points de contact des forces de l'ordre; la mise en place d'un réseau européen de points de contact public-privé réunissant les experts en cybercriminalité et les forces de l'ordre et d'autres actions de coopération du même type.
- ***Option 3***- mise à jour sélective des dispositions de la décision-cadre (nouvelle directive remplaçant cette dernière) pour répondre à la menace d'attaques à grande échelle contre des systèmes d'information («réseaux zombies») : cette option prévoit l'introduction d'une législation spécifique ciblée pour prévenir les attaques à grande échelle et s'accompagnerait de mesures non législatives en vue d'intensifier la coopération opérationnelle transfrontières contre ces attaques.
-

Option 4- adoption d'un corpus complet de législation européenne contre la cybercriminalité : cette option impliquerait une nouvelle législation européenne complète. Outre l'adoption des mesures non contraignantes prévues dans l'option 2 et la mise à jour mentionnée dans l'option 3, cette solution aborderait d'autres problèmes juridiques liés à l'utilisation de l'internet (comme la cyber-délinquance financière, les contenus illégaux sur l'internet, les collectes/stockages/transferts de preuves électroniques, …).

- ***Option 5*** : mise à jour de la convention du Conseil de l'Europe sur la cybercriminalité : cette option obligerait à renégocier une bonne partie de la convention actuelle, ce qui prendrait du temps et ne semble pas réaliste au vu du manque de volonté internationale de renégocier ladite convention.

L'option privilégiée est une combinaison entre des mesures non législatives (option 2) et une mise à jour sélective de la décision-cadre (option 3).

BASE JURIDIQUE : article 83, par. 1 du traité sur le fonctionnement de l'Union européenne (TFUE).

CONTENU : partant de la décision-cadre 2005/222/JAI qu'elle abroge, la proposition de directive apporte de nombreuses et importantes innovations qui peuvent se résumer comme suit :

S'agissant du droit pénal matériel en général, la proposition de directive:

- incrimine la production, la vente, l'acquisition en vue de l'utilisation, l'importation, la distribution ou la mise à disposition par d'autres moyens de dispositifs/outils utilisés pour commettre les infractions;
- prévoit des **circonstances aggravantes**:

  i. **la grande ampleur des attaques** – les réseaux zombies ou dispositifs similaires seraient incriminés en créant de nouvelles circonstances aggravantes, en ce sens que la mise en place d'un réseau zombies ou d'un dispositif similaire constituerait un facteur aggravant lors de la commission des infractions énumérées dans la décision-cadre existante;

  ii. **lorsque les attaques sont commises en dissimulant l'identité réelle de l'auteur** et en causant un préjudice au titulaire légitime de l'identité. Toutes ces dispositions devraient être conformes aux principes de légalité et de proportionnalité des infractions et sanctions pénales, et être compatibles avec la législation existante sur la protection des données à caractère personnel ;

- crée l'infraction d'«**interception illégale**» à savoir l'interception intentionnelle, par des moyens techniques, de transmissions non publiques de données informatiques vers un système d'information ou à partir ou à l'intérieur d'un tel système ;
- introduit des mesures pour **améliorer la coopération européenne** en matière de justice pénale en consolidant la structure existante des points de contact 24/7 : l'obligation de donner suite à une demande d'assistance émise par les points de contact opérationnels dans un certain délai est proposée. Cette mesure a pour but d'assurer que les points de contact indiquent dans un délai déterminé s'ils sont en mesure de répondre à la demande d'assistance et dans quel délai le point de contact demandeur peut attendre la solution au problème soumis. Le contenu exact des solutions n'est pas précisé;
- répond au besoin d'établir des **statistiques sur les infractions informatiques** en faisant obligation aux États membres de mettre en place un dispositif approprié d'enregistrement, de production et de communication de statistiques sur les infractions énumérées dans la décision-cadre existante et la nouvelle infraction d'«interception illégale».

Prise en compte de la « gravité » de l'infraction : dans les définitions des infractions pénales énumérées aux articles 3, 4, 5 (accès illégal à des systèmes d'information, atteinte à l'intégrité d'un système et atteinte à l'intégrité des données), la proposition directive contient une disposition qui permet de **n'incriminer que**

les «cas qui ne sont pas sans gravité» lors de la transposition de la directive en droit national. Cette flexibilité a pour but de permettre aux États membres de ne pas inclure les cas qui seraient *in abstracto* couverts par la définition de base, mais dont il est considéré qu'ils ne nuisent pas à l'intérêt juridique protégé, par exemple des actes commis par des jeunes gens qui veulent prouver leur savoir-faire en technologies de l'information. Cette possibilité de limiter la portée de l'incrimination ne devrait cependant pas conduire à l'introduction d'autres éléments constitutifs d'infraction que ceux déjà prévus par la directive, car il s'ensuivrait que seules les infractions commises dans des circonstances aggravantes seraient couvertes. Lors de la transposition, les États membres devraient notamment s'abstenir d'ajouter d'autres éléments constitutifs aux infractions de base, comme, par exemple, une intention particulière de tirer des revenus illicites d'une infraction ou l'existence d'une conséquence spécifique, comme un préjudice considérable.

INCIDENCE BUDGÉTAIRE : la proposition a une faible incidence sur le budget de l'Union. Plus de 90% du coût, estimé à 5.913.000 EUR, seraient supportés par les États membres et il est possible de demander un financement de l'Union pour réduire le coût.