Coopération judiciaire pénale: attaques visant les réseaux de communication et les systèmes d'information. Décision-cadre

2002/0086(CNS) - 19/04/2002 - Document de base législatif

OBJECTIF : rapprocher les règles pénales des États membres réprimant les attaques contre les systèmes d'information, afin notamment de contribuer à la lutte contre la criminalité organisée et le terrorisme, et renforcer la coopération judiciaire dans le domaine des infractions pénales liées aux attaques contre les systèmes d'information. CONTENU : les attaques contre les systèmes d'information constituent une menace pour la réalisation d'une société de l'information plus sûre et d'un espace de liberté, de sécurité et de justice (ELSJ). En vue de répondre à cette menace, la présente proposition de décision-cadre a pour objet de rapprocher les législations et les réglementations des États membres en matière de coopération policière et judiciaire pénale. Elle prévoit des règles minimales relatives aux éléments constitutifs des infractions pénales, tout particulièrement dans le domaine de la criminalité organisée et du terrorisme. Elle vise également à assurer la compatibilité des règles applicables dans les États membres en vue de faciliter et d'accélérer la coopération entre les autorités judiciaires. Aux fins de la présente proposition, les systèmes d'information couvrent les ordinateurs personnels autonomes, les agendas électroniques personnels, les téléphones mobiles, les intranets, les extranets, ainsi que les réseaux, serveurs et autres infrastructures d'Internet. L'intention n'est pas d'exiger que les États membres criminalisent des actes mineurs ou insignifiants. Seuls sont visés les actes graves. En particulier, la proposition n'affecte pas les droits à la vie privée ou à la protection des données et les obligations prévues par le droit communautaire (directives 95/46/CE et 97/66/CE, par exemple). Par conséquent, la proposition couvre uniquement les actes suivants : - accès non autorisé à des systèmes d'information. Cela couvre la notion de piratage qui consiste à accéder sans y être autorisé à un ordinateur ou à un réseau d'ordinateurs; - perturbation de systèmes d'information. L'un des moyens les plus connus de dégrader les services offerts sur Internet ou d'en dénier l'accès est une attaque par "déni de service" (DdS) visant à submerger les serveurs ou les fournisseurs de services Internet de messages générés automatiquement; - exécution de logiciels malveillants modifiant ou détruisant des données (virus). - interception malveillante des communications ("sniffing" ou reniflage); - présentation mensongère (l'usurpation de l'identité ou de l'adresse d'une autre personne sur Internet et son utilisation à des fins malveillantes, appelé "spoofing"). La proposition ne couvre pas seulement les actes visant les États membres. Elle s'applique également à des actes perpétrés sur le territoire de l'Union européenne et visant des systèmes d'information situés sur le territoire de pays tiers. Le rapprochement au niveau de l'Union devra tenir compte des travaux réalisés dans les enceintes internationales et s'inscrire dans la ligne des politiques communautaires actuelles. La proposition devrait permetre un rapprochement plus poussé des législations au sein de l'Union que cela n'aété possible dans d'autres enceintes internationales.