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

2010/0273(COD) - 04/07/2013 - Texte adopté du Parlement, 1ère lecture/lecture unique

Le Parlement européen a adopté par 541 voix pour, 91 voix contre et 9 abstentions, une résolution législative sur la proposition de directive du Parlement européen et du Conseil relative aux attaques visant les systèmes d'information et abrogeant la décision-cadre 2005/222/JAI du Conseil.

Le Parlement a arrêté sa position en première lecture suivant la procédure législative ordinaire. Les amendements adoptés en plénière sont le résultat d'un compromis négocié entre le Parlement européen et le Conseil. Ils modifient la proposition comme suit :

Objet de la directive : la directive vise à fixer les règles minimales concernant **la définition des infractions pénales et des sanctions en matière d'attaques visant les systèmes d'information**. Elle vise également à faciliter la prévention de ces infractions et à améliorer la coopération entre les autorités judiciaires et les autres autorités compétentes.

Définitions : une définition a été ajoutée pour définir le comportement ou l'accès "**sans droit**": il s'agit d' un accès, d'une atteinte à l'intégrité, d'une interception, ou de tout autre comportement non autorisé par le propriétaire ou autre détenteur de droits au système ou à une partie du système, ou non prévu par la législation nationale.

Une définition a également été introduite dans les considérants sur ce qu'il faut entendre par «**interception** » : celle-ci doit se comprendre (sans que cette liste soit limitative), comme l'écoute, le contrôle ou la surveillance du contenu des communications, et l'obtention du contenu des données, soit directement, au moyen de l'accès aux systèmes d'information et de leur utilisation, soit indirectement, au moyen de dispositifs d'écoute électroniques.

Atteinte illégale à l'intégrité d'un système : les États membres sont appelés à prendre les mesures nécessaires pour ériger en **infraction pénale punissable** le fait de provoquer une perturbation grave ou une interruption du fonctionnement d'un système d'information, en introduisant, transmettant, endommageant, effaçant, détériorant, altérant, supprimant ou rendant inaccessibles des données informatiques **lorsque l'acte est commis de manière intentionnelle** et sans droit, au moins dans les cas où les faits ne sont pas mineurs. Il en va de même pour une atteinte à l'intégrité des données ou en cas d' interception illégale au sens de la directive.

Incitation, participation, complicité et tentative : des mesures devront également être prévues pour faire en sorte d'ériger en infraction pénale punissable le fait d'inciter à commettre l'une des infractions visées à la directive, **d'y participer ou de s'en rendre complice**. Les États membres sont également appelés à faire en sorte d'ériger en infraction pénale punissable la simple **tentative** de commettre ces infractions.

Sanctions et peines : les **infractions visées à la directive seront passibles de peines suivantes** :

- peines d'emprisonnement maximales **d'au moins 2 ans**, si les faits ne sont pas mineurs ;
- peines d'emprisonnement maximales **d'au moins 3 ans**, si certaines infractions visées à la directive sont commises **de manière intentionnelle**, et si un nombre important de systèmes d'information sont atteints au moyen d'un outil conçu ou adapté à cette fin. ;
- peines d'emprisonnement maximales **d'au moins 5 ans**, si certaines des infractions visées à la directive sont commises :

- dans le cadre d'une organisation criminelle ; ou
- causent un préjudice considérable ; ou encore
- contre un système d'information faisant partie **d'une infrastructure critique**.

De manière générale, **des sanctions pénales sont prévues pour les cas où les faits ne sont pas mineurs**. Un considérant précise qu'il revient aux États membres de déterminer, en fonction de la loi et de la pratique nationales, ce qui constitue un cas mineur (par exemple, lorsque les dommages causés par l'infraction et/ou le risque qu'elle comporte pour les intérêts publics ou privés, comme pour l'intégrité d'un système informatique ou de données informatiques, ou pour l'intégrité, les droits ou les autres intérêts d'une personne, sont peu importants ou de nature telle qu'il n'est pas nécessaire d'appliquer des sanctions pénales dans le cadre du seuil légal ou d'engager la responsabilité pénale).

En outre, si certaines infractions sont commises par l'utilisation abusive des données à caractère personnel **d'une autre personne**, en vue de gagner la confiance d'une tierce partie, causant ainsi un préjudice au propriétaire légitime de l'identité, ces éléments pourront être considérés comme des **circonstances aggravantes**. Un considérant précise à cet effet que **l'usurpation d'identité** et d'autres infractions du même type nécessite **une action au niveau de l'UE** dans le cadre, à terme, d'un instrument horizontal global au niveau de l'UE.

Compétence: les États membres sont appelés à informer la Commission de leur décision **d'élargir leur compétence à l'égard des infractions** visées à la directive qui ont été commises **en dehors de leur territoire**, par exemple dans les cas suivants:

- si l'auteur de l'infraction réside habituellement sur son territoire; ou
- si l'infraction a été commise pour le compte d'une personne morale établie sur leur territoire.

Point de contact national : les États membres devront veiller à disposer **d'un point de contact national opérationnel** et à recourir au réseau existant de points de contact opérationnels, disponibles 24h/24 et 7jrs /7 et à mettre en place des procédures pour pouvoir, en cas de demandes urgentes, indiquer, dans un délai maximal de 8 heures, au moins si la demande d'aide sera satisfaite, ainsi que la forme et le délai estimé pour la réponse.

Collecte de données : des données comparables sur les infractions visées à la directive pourront être recueillies et transmises à des agences spécialisées comme Europol et l'Agence européenne chargée de la sécurité des réseaux et de l'information en fonction de leurs missions et de leurs besoins en information. L' objectif est de générer une vision plus complète du problème de la cybercriminalité et du niveau de sécurité des réseaux et de l'information au niveau de l'UE et de permettre ainsi de formuler des réponses plus efficaces.

Remplacement de la décision-cadre 2005/222/JAI : la directive remplacera la décision-cadre 2005/222 /JAI relative aux attaques visant des systèmes d'information.

Rapports : la Commission devra présenter au Parlement européen et au Conseil, au plus tard **4 ans à compter de l'adoption de la présente directive**, un rapport évaluant dans quelle mesure les États membres ont pris les dispositions nécessaires pour s'y conformer, accompagné, le cas échéant, de propositions législatives. À cet égard, la Commission devra également tenir compte des évolutions techniques et juridiques dans le domaine de la cybercriminalité, en particulier au regard du champ d'application de la directive.