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

2010/0273(COD) - 12/08/2013 - Acte final

OBJECTIF : rapprocher le droit pénal des États membres dans le domaine des attaques contre les systèmes d'information.

ACTE LÉGISLATIF : Directive 2013/40/UE du Parlement européen et du Conseil relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil.

CONTENU : la directive fixe des **règles minimales concernant la définition des infractions pénales et les sanctions** en matière d'attaques contre 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**.

Infractions : **lorsqu'il ne s'agit pas de cas mineurs**, et qu'ils sont commis **de manière intentionnelle et sans droit**, les actes suivants sont considérés comme des infractions punissables par des sanctions pénales au sens de la directive :

- **accès illégal à des systèmes d'information** : accès à tout ou partie d'un système d'information en violation d'une mesure de sécurité ;
- **atteinte illégale à l'intégrité d'un système** : le fait de provoquer une perturbation grave ou une interruption du fonctionnement d'un système d'information, en introduisant, en transmettant, en endommageant, en effaçant, en détériorant, en altérant, en supprimant ou en rendant inaccessibles des données informatiques ;
- **atteinte illégale à l'intégrité des données** : le fait d'effacer, d'endommager, de détériorer, d' altérer, de supprimer ou de rendre inaccessibles des données informatiques d'un système d' information ;
- **interception illégale** : l'interception, effectuée par des moyens techniques, de transmissions non publiques de données informatiques à destination, en provenance ou à l'intérieur d'un système d' information, y compris les émissions électromagnétiques provenant d'un système d'information transportant de telles données informatiques ;
- **outils utilisés pour commettre les infractions** : la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition intentionnelles d'un des outils suivants dans l'intention de l'utiliser pour commettre l'une des infractions visées ci-avant : i) un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions visées ; ii) un mot de passe, un code d'accès ou des données informatiques similaires permettant d'accéder à tout ou partie d'un système d'information.

Incitation, participation et complicité, et tentative : la directive appelle les États membres à veiller à ériger en infraction pénale :

- le fait d'inciter à commettre les infractions visées à la directive, d'y participer ou de s'en rendre complice ;
- **la seule tentative de commettre une atteinte illégale à l'intégrité d'un système ou une atteinte illégale à l'intégrité des données**.

Sanctions : les infractions visées à la directive seraient passibles des peines suivantes :

- peines d'emprisonnement maximales **d'au moins 2 ans**, si les infractions visées à la directive ne sont pas mineures ;
- peines d'emprisonnement maximales **d'au moins 3 ans**, si les infractions d'atteinte illégale à l'intégrité d'un système ou d'atteinte illégale à l'intégrité des données 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 les infractions d'atteinte illégale à l'intégrité d'un système ou d'atteinte illégale à l'intégrité des données sont commises i) dans le cadre d'une organisation criminelle ; ou ii) causent un préjudice considérable ; ou encore iii) sont commises contre un système d'information faisant partie d'une infrastructure critique.

Si les infractions liées à l'atteinte illégale à l'intégrité d'un système ou à l'intégrité des données 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 seraient considérés comme des circonstances aggravantes à moins que ces circonstances ne soient déjà couvertes par une autre infraction punissable en vertu du droit national.

Un considérant précise à cet effet que la mise en place de mesures efficaces contre l'usurpation d'identité et d'autres infractions liées à l'identité constitue un autre élément important d'une approche intégrée contre la cybercriminalité. La nécessité de mener une action au niveau de l'Union contre ce type de comportement criminel pourrait également être envisagée à un stade ultérieur.

Responsabilité des personnes morales : des dispositions sont prévues pour faire en sorte que les personnes morales puissent être tenues pour responsables des infractions visées au texte de la directive et soient sanctionnées.

Compétence : des dispositions sont également prévues pour que les États membres établissent leur compétence à l'égard des infractions visées à la directive. Il est en outre précisé qu'étant donné que les systèmes d'information modernes ont un **caractère transnational et ne connaissent pas de frontières**, les attaques lancées contre eux ont également une dimension transfrontière, ce qui rend nécessaire la fixation de mesures complémentaires pour rapprocher le droit pénal dans ce domaine.

Point de contact national : il est prévu que les États membres veillent 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 : un considérant précise qu'il est nécessaire de recueillir des données comparables sur les infractions prévues à la directive. Des données pertinentes devraient être mises à la disposition des agences et organes spécialisés compétents de l'Union, comme Europol et ENISA, en fonction de leurs missions et de leurs besoins en information, afin d'avoir une vision plus complète du problème de la cybercriminalité et du niveau de sécurité des réseaux et de l'information au niveau de l'Union et permettre ainsi de formuler une réponse plus efficace. Dans ce contexte, les États membres devraient transmettre à Europol et à son Centre européen de lutte contre la cybercriminalité des informations sur le mode opératoire des auteurs d'infractions, afin que ces agences puissent établir des évaluations de la menace et des analyses stratégiques en matière de cybercriminalité, conformément à la décision 2009/371/JAI du Conseil.

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

Rapports : la Commission est appelée à présenter au Parlement européen et au Conseil, au plus tard pour le 4 septembre 2017, 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.

ENTRÉE EN VIGUEUR : 03.09.2014.

TRANSPOSITION : 04.09.2015.