Informations de base

2010/0273(COD) COD - Procédure législative ordinaire (ex-procedure codécision) Directive	Procédure terminée
Coopération judiciaire pénale: lutte contre attaques visant les systèmes d'information Abrogation 2002/0086(CNS) **Subject** 3.30.06 Technologies de l'information et de la communication, technologies numériques 3.30.07 Cybersécurité, politique cyberespace 3.30.25 Réseaux mondiaux et société de l'information, internet 7.40.04 Coopération judiciaire en matière pénale	

Acteurs principaux

Parlement européen

Commission au fond	Rapporteur(e)	Date de nomination
LIBE Libertés civiles, justice et affaires intérieures	HOHLMEIER Monika (PPE)	09/12/2010
	Rapporteur(e) fictif/fictive PICKART ALVARO Alexander Nuno (ALDE) ALBRECHT Jan Philipp (Verts/ALE) KIRKHOPE Timothy (ECR) VERGIAT Marie-Christine (GUE/NGL)	

Commission pour avis	Rapporteur(e) pour avis	Date de nomination
AFET Affaires étrangères	OJULAND Kristiina (ALDE)	29/03/2011
BUDG Budgets	La commission a décidé de ne pas donner d'avis.	
ITRE Industrie, recherche et énergie	EHLER Christian (PPE)	24/11/2010

Conseil de l'Union européenne

Formation du Conseil	Réunions	Date

	Justice et affaires intérieures(JAI)	3096	2011-06-09

Commission européenne	DG de la Commission	Commissaire
	Migration et affaires intérieures	MALMSTRÖM Cecilia

Evénements clés

Date	Evénement	Référence	Résumé
30/09/2010	Publication de la proposition législative	COM(2010)0517	Résumé
07/10/2010	Annonce en plénière de la saisine de la commission, 1ère lecture		
09/06/2011	Débat au Conseil		Résumé
06/06/2013	Vote en commission,1ère lecture		
19/06/2013	Dépôt du rapport de la commission, 1ère lecture	A7-0224/2013	Résumé
03/07/2013	Débat en plénière		
04/07/2013	Décision du Parlement, 1ère lecture	T7-0321/2013	Résumé
04/07/2013	Résultat du vote au parlement		
22/07/2013	Adoption de l'acte par le Conseil après la 1ère lecture du Parlement		
12/08/2013	Signature de l'acte final		
12/08/2013	Fin de la procédure au Parlement		
14/08/2013	Publication de l'acte final au Journal officiel		

Informations techniques

Référence de la procédure	2010/0273(COD)
Type de procédure	COD - Procédure législative ordinaire (ex-procedure codécision)
Sous-type de procédure	Note thématique
Instrument législatif	Directive
Modifications et abrogations	Abrogation 2002/0086(CNS)
Base juridique	Traité sur le fonctionnement de l'Union européenne TFEU 083-p1-a1
État de la procédure	Procédure terminée
Dossier de la commission	LIBE/7/04091

Portail de documentation

Parlement Européen

Type de document	Commission	Référence	Date	Résumé

Avis de la commission	ITRE	PE472.192	11/11/2011	
Projet de rapport de la commission		PE476.089	24/11/2011	
Avis de la commission	AFET	PE469.848	28/11/2011	
Amendements déposés en commission		PE480.665	27/01/2012	
Rapport déposé de la commission, 1ère lecture/lecture unique		A7-0224/2013	19/06/2013	Résumé
Texte adopté du Parlement, 1ère lecture/lecture unique		T7-0321/2013	04/07/2013	Résumé

Conseil de l'Union

Type de document	Référence	Date	Résumé
Projet d'acte final	00038/2012/LEX	12/08/2013	

Commission Européenne

Type de document	Référence	Date	Résumé
Document de base législatif	COM(2010)0517	30/09/2010	Résumé
Document annexé à la procédure	SEC(2010)1122	30/09/2010	
Document annexé à la procédure	SEC(2010)1123	30/09/2010	
Réaction de la Commission sur le texte adopté en plénière	SP(2013)625	24/09/2013	
Document de suivi	COM(2017)0474	13/09/2017	Résumé

Parlements nationaux

Type de document	Parlement /Chambre	Référence	Date	Résumé
Contribution	IT_SENATE	COM(2010)0517	19/11/2010	
Contribution	PT_PARLIAMENT	COM(2010)0517	01/12/2010	
Contribution	IT_CHAMBER	COM(2010)0517	16/12/2010	

Autres Institutions et organes

Institution/organe	Type de document	Référence	Date	Résumé
EESC	Comité économique et social: avis, rapport	CES0816/2011	04/05/2011	

Informations complémentaires

Source	Document	Date

Parlements nationaux	IPEX	
Commission européenne	EUR-Lex	

Acte final	
Directive 2013/0040 JO L 218 14.08.2013, p. 0008	Résumé

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.

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.

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

2010/0273(COD) - 13/09/2017 - Document de suivi

La Commission a présenté un rapport évaluant dans quelle mesure les États membres ont pris les dispositions nécessaires pour se conformer à la directive 2013/40/UE relative aux attaques contre les systèmes d'information.

Pour rappel, la directive vise à rapprocher le droit pénal des États membres en matière d'attaques contre les systèmes d'information et à améliorer la coopération entre les autorités compétentes. À cette fin, la directive fixe des règles minimales concernant la définition des infractions pénales et les sanctions en matière d'attaques contre les systèmes d'information et impose l'existence de points de contact opérationnels 24 heures sur 24 et 7 jours sur 7.

À la date limite de transposition, **22 États membres avaient notifié à la Commission l'achèvement de la transposition** de la directive. Au 31 mai 2017, des procédures d'infraction pour non-communication de mesures nationales de transposition à l'encontre de trois États membres (BE, BG et IE) étaient toujours en cours. La Commission reconnaît toutefois les efforts déployés par les États membres pour transposer la directive.

L'analyse contenue dans le présent rapport est basée sur les informations communiquées par les États membres au plus tard le 31 mai 2017.

Progrès accomplis: le rapport conclut que la directive a permis d'accomplir **des progrès réels en matière de criminalisation des cyberattaques** à un niveau comparable dans tous les États membres, ce qui facilite la coopération transfrontière entre les autorités répressives qui enquêtent sur ce type d' infractions.

Les États membres ont modifié leurs codes pénaux et leur législation applicable. Ils ont **rationalisé leurs procédures** et ont mis en place ou amélioré leurs programmes de coopération.

Améliorations nécessaires: la Commission confirme toutefois que **beaucoup reste à faire** pour que la directive atteigne son plein potentiel. Les principales améliorations à mettre en œuvre par les États membres devraient concerner en particulier:

- **l'utilisation des définitions** des termes «système d'information», «données informatiques», «personne morale» et «sans droit» fournies par la directive: seuls deux pays ont introduit une législation couvrant tous les aspects de ces définitions;
- **l'inclusion de l'ensemble des possibilités qui caractérisent les actions liées aux infractions pénales spécifiques** (accès illégal à des systèmes d' information ; atteinte illégale à l'intégrité d'un système et à l'intégrité des données ; interception illégale des données informatiques : outils, tels que les programmes informatiques ou les codes d'accès, utilisés pour commettre les infractions) ;
- **la mise en place de normes communes en matière de sanctions pour les cyberattaques** (niveau minimal général de la peine maximale ; sanctions lorsqu'un nombre important de systèmes d'information est atteint ; infractions commises par une organisation criminelle ; préjudice grave causé ; implication de systèmes d'information d'infrastructures critiques dans les infractions ; usurpation d'identité ; responsabilité des personnes morales).

D'autres problèmes semblent liés à la mise en œuvre des dispositions administratives concernant la mise à disposition par États membres des **canaux de communication appropriés** afin de faciliter la notification aux autorités nationales compétentes des infractions, ainsi qu'au suivi et aux **statistiques** concernant les infractions relevant de la directive

Perspectives: la Commission indique qu'elle continuera de **soutenir les États membres** dans leur mise en œuvre de la directive et qu'elle fournira aux États membres des occasions supplémentaires de recenser et d'échanger leurs bonnes pratiques au cours du second semestre 2017.

La Commission **ne voit pas la nécessité proposer des modifications de la directive**. Elle envisage plutôt des mesures visant à **améliorer l'accès transfrontière aux preuves électroniques** dans le cadre des enquêtes criminelles, notamment en proposant des mesures législatives au début de 2018. Elle étudie également le rôle que joue le chiffrement dans les enquêtes criminelles et présentera ses conclusions sur le sujet d'ici octobre 2017.

Enfin, la Commission s'attachera à ce que **la transposition soit finalisée** dans l'ensemble de l'Union et à ce que les dispositions soient correctement appliquées.

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

2010/0273(COD) - 19/06/2013 - Rapport déposé de la commission, 1ère lecture/lecture unique

La commission des libertés civiles, de la justice et des affaires intérieures a adopté le rapport de Monika HOHLMEIER (PPE, DE) 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.

La commission parlementaire recommande que la position du Parlement européen adoptée en première lecture suivant la procédure législative ordinaire modifie la proposition de la Commission 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.

Á noter également que dans les considérants, une définition a été introduite 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 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 sans gravité. 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, 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 **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 : dans un considérant, il est précisé que des sanctions pénales sont au moins prévues pour les cas où **les faits ne sont pas sans gravité**. Ils peuvent déterminer, en fonction de la loi et de la pratique nationales, ce qui constitue un cas sans gravité (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 tout état de cause, 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 sans gravité ;
- 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**.

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 : il est précisé qu'il est nécessaire de recueillir des données comparables sur les infractions visées à la directive et de les transmettre 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 : il est clairement spécifié que la directive vise à remplacer la décision-cadre 2005/222/JAI relative aux attaques visant des systèmes d'information.

Rapports : la Commission devra enfin 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.

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.

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.