



PARLEMENT EUROPÉEN

2009 - 2014

---

*Commission des affaires étrangères*

---

**2013/0027(COD)**

6.12.2013

## **AVIS**

de la commission des affaires étrangères

à l'intention de la commission du marché intérieur et de la protection des consommateurs

sur la proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union  
(COM(2013)0048 – C7-0035/2013 – 2013/0027(COD))

Rapporteure pour avis: Ana Gomes

PA\_Legam

## AMENDEMENTS

La commission des affaires étrangères invite la commission du marché intérieur et de la protection des consommateurs, compétente au fond, à incorporer dans son rapport les amendements suivants:

### Amendement 1

#### Proposition de directive Considérant 1

##### *Texte proposé par la Commission*

(1) Les réseaux et les services et systèmes informatiques jouent un rôle crucial dans la société. Leur fiabilité et leur sécurité sont essentielles à l'activité économique et au bien-être social et notamment au bon fonctionnement du marché intérieur.

##### *Amendement*

(1) Les réseaux et les services et systèmes informatiques jouent un rôle crucial dans la société. Leur fiabilité et leur sécurité sont essentielles à l'activité économique et au bien-être social et notamment au bon fonctionnement du marché intérieur, *ainsi qu'à la sécurité extérieure de l'Union.*

### Amendement 2

#### Proposition de directive Considérant 2

##### *Texte proposé par la Commission*

(2) L'ampleur et la fréquence des incidents de sécurité, d'origine malveillante ou accidentelle, ne cessent de croître et elles représentent une menace considérable pour le fonctionnement des réseaux et des systèmes informatiques. Ces incidents peuvent nuire à l'exercice d'activités économiques, entraîner des pertes financières importantes, entamer la confiance des utilisateurs et porter un grand préjudice à l'économie de l'UE dans son ensemble.

##### *Amendement*

(2) L'ampleur et la fréquence des incidents de sécurité, d'origine malveillante ou accidentelle, ne cessent de croître et elles représentent une menace considérable pour le fonctionnement des réseaux et des systèmes informatiques. Ces incidents peuvent nuire à l'exercice d'activités économiques, entraîner des pertes financières importantes, entamer la confiance des utilisateurs, porter un grand préjudice à l'économie de l'UE dans son ensemble *et, en fin de compte, mettre en péril le bien-être des citoyens de l'Union ainsi que la capacité des États membres à se protéger et à assurer la sécurité des infrastructures critiques.*

### Amendement 3

#### Proposition de directive Considérant 2 bis (nouveau)

*Texte proposé par la Commission*

*Amendement*

*(2 bis) La clause de solidarité, instituée par l'article 222 du traité FUE, représente le cadre approprié pour une entraide et une action concertée entre États membres de l'Union en cas d'attaque terroriste ou d'activité criminelle mettant en péril la sécurité des réseaux et de l'information. De la même manière, la clause de défense mutuelle, établie à l'article 42, paragraphe 7, du traité UE, constitue le cadre d'action au sein de l'Union au cas où un État membre serait l'objet d'une agression armée portant atteinte à la sécurité des réseaux et de l'information. Le cas échéant, il convient d'appliquer de manière complémentaire l'article 222 du traité FUE et l'article 42, paragraphe 7, du traité UE.*

### Amendement 4

#### Proposition de directive Considérant 2 bis (nouveau)

*Texte proposé par la Commission*

*Amendement*

*(2 bis) Un grand nombre d'incidents informatiques sont imputables à un défaut de résistance et de robustesse des infrastructures de réseau privées et publiques, à des bases de données mal protégées ou sécurisées et à d'autres failles dans les infrastructures d'information critiques. Seuls quelques États membres considèrent la protection de leurs réseaux et systèmes d'information, ainsi que des données associées, comme faisant partie de leurs obligations respectives de vigilance, ce qui explique le manque d'investissements*

*dans des technologies de pointe en matière de sécurité, mais aussi dans la formation et dans l'élaboration de lignes directrices appropriées.*

## Amendement 5

### Proposition de directive Considérant 3

*Texte proposé par la Commission*

(3) Les systèmes d'information numériques, et notamment l'internet, sont des instruments de communication sans frontières qui revêtent une importance essentielle pour la circulation transfrontières des biens, des services et des personnes. En raison de ce caractère transnational, toute perturbation importante de ces systèmes dans un État membre peut avoir une incidence sur d'autres États membres et sur l'UE dans son ensemble. La résilience et la stabilité des réseaux et systèmes informatiques sont donc essentielles au fonctionnement harmonieux du marché intérieur.

*Amendement*

(3) Les systèmes d'information numériques, et notamment l'internet, sont des instruments de communication sans frontières qui revêtent une importance essentielle pour la circulation transfrontières des biens, des services et des personnes. En raison de ce caractère transnational, toute perturbation importante de ces systèmes dans un État membre peut avoir une incidence sur d'autres États membres et sur l'UE dans son ensemble. La résilience et la stabilité des réseaux et systèmes informatiques sont donc essentielles au fonctionnement harmonieux du marché intérieur, *et capitales pour la sécurité intérieure et extérieure de l'Union. Il conviendrait dès lors d'insister, tant dans le cadre de la stratégie de sécurité intérieure de l'Union européenne que de la stratégie européenne de sécurité, sur la nécessité d'améliorer la sécurité des réseaux et de l'information, en particulier dans la perspective de la révision de ces documents.*

## Amendement 6

### Proposition de directive Considérant 3 bis (nouveau)

*Texte proposé par la Commission*

*Amendement*

*(3 bis) La sensibilisation et la formation des utilisateurs des technologies de*

*l'information et de la communication aux bonnes pratiques relatives à la sécurisation des données à caractère personnel et au maintien durable des services de communication devraient constituer la base de toute stratégie globale de cybersécurité.*

## **Amendement 7**

### **Proposition de directive Considérant 4 bis (nouveau)**

*Texte proposé par la Commission*

*Amendement*

*(4 bis) La coopération et la coordination entre les autorités européennes compétentes et le HR/VP, chargé de la politique étrangère et de sécurité commune et de la politique de sécurité et de défense commune, ainsi qu'avec le coordinateur de l'UE pour la lutte contre le terrorisme, devraient être garanties dans tous les cas où les risques peuvent apparaître comme étant de nature extérieure et terroriste.*

## **Amendement 8**

### **Proposition de directive Considérant 4 ter (nouveau)**

*Texte proposé par la Commission*

*Amendement*

*(4 ter) L'échange de renseignements et d'informations sensibles entre les États membres ainsi qu'entre ces derniers et les autorités compétentes de l'Union devrait être renforcé et s'ancrer dans les principes de confiance, de solidarité et de coopération. Tout plan d'action visant à améliorer la sécurité des réseaux et des systèmes devrait dès lors avoir pleinement recours aux structures existantes de l'Union, telles que le Centre de situation (SITCEN) et le Centre d'analyse du*

*renseignement (INTCEN), et veiller à une bonne coordination entre toutes les structures concernées par la sécurité des informations présentant un caractère sensible pour la sécurité intérieure et extérieure de l'Union.*

## **Amendement 9**

### **Proposition de directive**

#### **Considérant 4 quater (nouveau)**

*Texte proposé par la Commission*

*Amendement*

*(4 quater) La coopération et l'échange d'informations, au niveau mondial, avec les partenaires internationaux appropriés, sont cruciaux pour assurer l'efficacité de la stratégie de cybersécurité et la pertinence des actions destinées à améliorer la sécurité des réseaux et de l'information au sein de l'Union, eu égard au caractère transnational de la menace.*

## **Amendement 10**

### **Proposition de directive**

#### **Considérant 8 bis (nouveau)**

*Texte proposé par la Commission*

*Amendement*

*(8 bis) Les mesures de sécurité doivent respecter les droits fondamentaux auxquels souscrivent l'Union européenne et ses États membres conformément aux articles 2, 6 et 21 du traité FUE, tels que la liberté d'expression, la protection des données et la protection de la vie privée. Les droits à la vie privée et à la protection des données sont inscrits dans la charte de l'Union européenne et à l'article 16 du traité FUE.*

## Amendement 11

### Proposition de directive Considérant 11 bis (nouveau)

*Texte proposé par la Commission*

*Amendement*

***(11 bis) Tous les États membres doivent axer les stratégies nationales de sécurité du cyberspace sur la protection des systèmes d'information et de données connexes et considérer que la protection de cette infrastructure critique fait partie de leur obligation de vigilance respective. Tous les États membres devraient adopter et mettre en œuvre des stratégies, des lignes directrices et des instruments garantissant des niveaux raisonnables de protection contre des niveaux raisonnablement identifiables de menaces, les coûts et les charges liés à cette protection étant proportionnés aux dommages probables subis par les parties concernées. Tous les États membres devraient prendre des mesures appropriées pour obliger les personnes morales relevant de leur compétence à protéger les données à caractère personnel dont elles ont la charge.***

## Amendement 12

### Proposition de directive Considérant 16

*Texte proposé par la Commission*

*Amendement*

(16) Pour garantir la transparence et informer correctement la population et les acteurs du marché de l'UE, les autorités compétentes devraient créer un site web commun destiné à la publication d'informations non confidentielles sur les incidents et les risques.

(16) Pour garantir la transparence et informer correctement la population et les acteurs du marché de l'UE, les autorités compétentes devraient créer un site web commun destiné à la publication d'informations non confidentielles sur les incidents et les risques. ***Toute publication de données à caractère personnel sur ce site web devrait être limitée au strict nécessaire et être aussi anonyme que***



*possible.*

### **Amendement 13**

#### **Proposition de directive Considérant 30 bis (nouveau)**

*Texte proposé par la Commission*

*Amendement*

*(30 bis) La présente directive est sans préjudice de l'acquis de l'Union relatif à la protection des données. Les données à caractère personnel utilisées en application des dispositions de la présente directive devraient être strictement limitées aux seules données personnelles minimales nécessaires, n'être communiquées qu'aux acteurs strictement nécessaires et être aussi anonymes que possible, voire totalement anonymes.*

### **Amendement 14**

#### **Proposition de directive Considérant 32 bis (nouveau)**

*Texte proposé par la Commission*

*Amendement*

*(32 bis) La présente directive (directive sur la SRI) s'applique sans préjudice de l'adoption nécessaire d'une législation sur les principes généraux de protection des données au niveau de l'Union.*

### **Amendement 15**

#### **Proposition de directive Considérant 34 bis (nouveau)**

*Texte proposé par la Commission*

*Amendement*

*(34 bis) Il est nécessaire de réglementer au niveau de l'Union européenne la vente, la fourniture, le transfert ou l'exportation à destination de pays tiers d'équipements*

*ou de logiciels destinés essentiellement à la surveillance ou à l'interception des communications internet et téléphoniques sur des réseaux mobiles ou fixes, et la fourniture d'une assistance pour installer, exploiter ou mettre à jour un tel équipement ou logiciel. Il est impératif que la Commission élabore dans les meilleurs délais des dispositions législatives empêchant les entreprises européennes d'exporter de tels biens à double usage vers des régimes non démocratiques, autoritaires et répressifs.*

## **Amendement 16**

### **Proposition de directive**

#### **Article 1 – paragraphe 2 – point b**

*Texte proposé par la Commission*

(b) elle crée un mécanisme de coopération entre les États membres, destiné à garantir une application uniforme de la présente directive dans l'Union et, le cas échéant, un traitement et une intervention coordonnés et efficaces en cas de risques et d'incidents touchant les réseaux et systèmes informatiques;

*Amendement*

(b) elle crée un mécanisme de coopération entre les États membres, destiné à garantir une application uniforme de la présente directive dans l'Union et, le cas échéant, un traitement et une intervention coordonnés, efficaces et efficaces en cas de risques et d'incidents touchant les réseaux et systèmes informatiques;

## **Amendement 17**

### **Proposition de directive**

#### **Article 3 – paragraphe 1 – point b**

*Texte proposé par la Commission*

(b) *tout dispositif isolé ou* tout ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données informatiques, ainsi que

*Amendement*

(b) tout ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données informatiques, ainsi que

## Amendement 18

### Proposition de directive

#### Article 3 – paragraphe 2 bis (nouveau)

*Texte proposé par la Commission*

*Amendement*

*(2 bis) "résilience d'un système", la capacité d'un réseau et d'un système informatique à résister à un incident et à retrouver sa pleine capacité opérationnelle après celui-ci, que l'incident relève du dysfonctionnement technique, de la coupure de courant, de l'incident de sécurité ou d'une autre catégorie encore;*

## Amendement 19

### Proposition de directive

#### Article 3 – paragraphe 8 – point b

*Texte proposé par la Commission*

*Amendement*

(b) un opérateur d'infrastructure critique essentielle au maintien de fonctions économiques et sociétales vitales dans le domaine de l'énergie, des transports, des services bancaires, des bourses de valeurs *et* de la santé, énumérées dans une liste non exhaustive qui figure à l'annexe II.

(b) un opérateur d'infrastructure critique essentielle au maintien de fonctions économiques et sociétales vitales dans le domaine de l'énergie, des transports, des services bancaires, des bourses de valeurs, de la santé, *de la sécurité et de la défense*, énumérées dans une liste non exhaustive qui figure à l'annexe II.

## Amendement 20

### Proposition de directive

#### Article 3 – paragraphe 8 – point b bis (nouveau)

*Texte proposé par la Commission*

*Amendement*

*(b bis) un fournisseur de dispositifs, de réseaux et de systèmes informatiques tels que définis au paragraphe 1, ou de leurs composants, qui sont vitaux pour le maintien d'un niveau élevé commun de sécurité des réseaux et de l'information.*

## Amendement 21

### Proposition de directive Article 6 – paragraphe 1

*Texte proposé par la Commission*

1. Chaque État membre désigne une autorité nationale civile compétente en matière de sécurité des réseaux et systèmes informatiques (l'"autorité compétente").

*Amendement*

1. Chaque État membre désigne une autorité nationale civile compétente en matière de sécurité des réseaux et systèmes informatiques (l'"autorité compétente").

## Amendement 22

### Proposition de directive Article 7 – paragraphe 1

*Texte proposé par la Commission*

1. Chaque État membre met en place une équipe d'intervention en cas d'urgence informatique (ci-après «CERT») chargée de la gestion des incidents et des risques selon un processus bien défini, et qui se conforme aux exigences énumérées au point (1) de l'annexe I. Une CERT peut être établie au sein de l'autorité compétente.

*Amendement*

1. Chaque État membre met en place **au moins** une équipe d'intervention en cas d'urgence informatique (ci-après "CERT") chargée de la gestion des incidents et des risques selon un processus bien défini, et qui se conforme aux exigences énumérées au point (1) de l'annexe I. Une CERT peut être établie au sein de l'autorité compétente.

## Amendement 23

### Proposition de directive Article 8 – paragraphe 3 – point f bis (nouveau)

*Texte proposé par la Commission*

*Amendement*

***(f bis) informent, lorsque la nature du risque ou de la menace concernés le justifient, le coordinateur de l'UE pour la lutte contre le terrorisme sous forme de rapports, et peuvent lui demander qu'il prête assistance en produisant une analyse des travaux préparatoires et des actions du réseau de coopération;***

## Amendement 24

### Proposition de directive Article 9 – paragraphe 1 bis (nouveau)

*Texte proposé par la Commission*

*Amendement*

***(1 bis) Les données à caractère personnel sont communiquées aux seuls destinataires qui ont besoin de les traiter pour mener à bien leurs tâches, conformément à une base juridique appropriée. Les données communiquées se limitent à celles nécessaires à l'accomplissement de ces missions. Le respect du principe de limitation de la finalité est garanti. Le délai de conservation de ces données est spécifié pour les objectifs fixés dans la présente directive.***

## Amendement 25

### Proposition de directive Article 10 – paragraphe 3

*Texte proposé par la Commission*

*Amendement*

3. La Commission peut, à la demande d'un État membre ou de sa propre initiative, demander à un État membre de fournir toute information pertinente concernant un risque ou un incident particulier.

3. La Commission peut, à la demande d'un État membre ou de sa propre initiative, demander à un État membre de fournir toute information pertinente concernant un risque ou un incident particulier, ***conformément aux dispositions du règlement général sur la protection des données.***

## **Amendement 26**

### **Proposition de directive**

#### **Article 13 – alinéa -1 bis (nouveau)**

*Texte proposé par la Commission*

*Amendement*

***(-1 bis) Le HR/VP veille à l'intégration, dans les actions extérieures de l'Union (en particulier dans les relations avec les pays tiers), des aspects liés à la cybersécurité. L'objectif d'une telle démarche est d'intensifier l'échange des enseignements tirés de l'expérience et la coopération en matière de cybersécurité.***

## **Amendement 27**

### **Proposition de directive**

#### **Article 13 – alinéa -1 ter (nouveau)**

*Texte proposé par la Commission*

*Amendement*

***(-1 ter) Le Conseil et la Commission, dans le cadre de leurs relations avec les pays tiers et des accords de coopération conclus avec eux, en particulier lorsque la coopération porte sur les technologies, insistent sur le respect d'un socle minimum de normes quant à la sécurité des systèmes informatiques.***

## **Amendement 28**

### **Proposition de directive**

#### **Article 20 – titre**

*Texte proposé par la Commission*

*Amendement*

Examen

***Rapports et examen***

## Amendement 29

### Proposition de directive

#### Article 20 – alinéa -1 bis (nouveau)

*Texte proposé par la Commission*

*Amendement*

***(-1 bis) La Commission présente au Parlement européen et au Conseil un rapport annuel concernant les incidents et les mesures qui ont été portés à sa connaissance en application de la présente directive.***

## Amendement 30

### Proposition de directive

#### Annexe I – point 1 – sous-point b

*Texte proposé par la Commission*

*Amendement*

(b) La CERT doit appliquer et gérer des mesures de sécurité pour assurer la confidentialité, l'intégrité, la disponibilité et l'authenticité des informations qu'elle reçoit et qu'elle traite.

(b) La CERT doit appliquer et gérer des mesures de sécurité pour assurer la confidentialité, l'intégrité, la disponibilité et l'authenticité des informations qu'elle reçoit et qu'elle traite, ***dans le respect des exigences en matière de protection des données.***

## Amendement 31

### Proposition de directive

#### Annexe II – sous-titre 2 (visés à l'article 3, paragraphe 8, point b) – paragraphe 5 bis (nouveau)

*Texte proposé par la Commission*

*Amendement*

***(5 bis) Secteur de la sécurité et de la défense: opérateurs économiques prestataires de travaux ou de services visés par la directive 2009/81/CE, en particulier à son article 46.***

## PROCÉDURE

<b>Titre</b>	Niveau élevé commun de sécurité des réseaux et de l'information dans l'Union
<b>Références</b>	COM(2013)0048 – C7-0035/2013 – 2013/0027(COD)
<b>Commission compétente au fond</b> Date de l'annonce en séance	IMCO 15.4.2013
<b>Avis émis par</b> Date de l'annonce en séance	AFET 15.4.2013
<b>Rapporteur(e) pour avis</b> Date de la nomination	Ana Gomes 19.2.2013
<b>Examen en commission</b>	18.9.2013
<b>Date de l'adoption</b>	5.12.2013
<b>Résultat du vote final</b>	+: 31 -: 3 0: 8
<b>Membres présents au moment du vote final</b>	Elmar Brok, Jerzy Buzek, Mark Demesmaeker, Marietta Giannakou, Ana Gomes, Andrzej Grzyb, Anna Ibrisagic, Jelko Kacin, Tunne Kelam, Nicole Kiil-Nielsen, Andrey Kovatchev, Eduard Kukan, Marusya Lyubcheva, Annemie Neyts-Uyttebroeck, Norica Nicolai, Raimon Obiols, Kristiina Ojuland, Ria Oomen-Ruijten, Ioan Mircea Paşcu, Alojz Peterle, Mirosław Piotrowski, Bernd Posselt, Hans-Gert Pöttering, Cristian Dan Preda, Libor Rouček, Tokia Saïfi, José Ignacio Salafranca Sánchez-Neyra, György Schöpflin, Werner Schulz, Marek Siwiec, Charles Tannock, Geoffrey Van Orden, Nikola Vuljanić, Boris Zala
<b>Suppléant(s) présent(s) au moment du vote final</b>	Marije Cornelissen, Barbara Lochbihler, Doris Pack, Marietje Schaake, Indrek Tarand, Ivo Vajgl, Paweł Zalewski
<b>Suppléant(s) (art. 187, par. 2) présent(s) au moment du vote final</b>	Hiltrud Breyer