COMMISSION
EUROPÉENNE

Bruxelles, le 30.5.2016
COM(2016) 363 final

2013/0027 (COD)

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN

conformément à l'article 294, paragraphe 6, du traité sur le fonctionnement de l'Union européenne

concernant la

position du Conseil sur l'adoption d'une directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union

(Texte présentant de l'intérêt pour l'EEE)

2013/0027 (COD)

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN

conformément à l'article 294, paragraphe 6, du traité sur le fonctionnement de l'Union européenne

concernant la

position du Conseil sur l'adoption d'une directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union

(Texte présentant de l'intérêt pour l'EEE)

1. CONTEXTE

Date de transmission de la proposition au Parlement européen et au Conseil [COM(2013) 48 – 2013/0027 (COD)]:	7.2.2013
Date de l'avis du Comité économique et social européen:	22.5.2013
Date de la position du Parlement européen en première lecture:	13.3.2014
Date de l'adoption de la position du Conseil:	17.5.2016

2. OBJET DE LA PROPOSITION DE LA COMMISSION

Premièrement, la proposition exige de tous les États membres qu'ils mettent en place un minimum de moyens au niveau national:

- en établissant des autorités compétentes dans le domaine de la sécurité des réseaux et de l'information (SRI);
- en mettant sur pied des centres de réponse aux incidents de sécurité informatique (CSIRT);
- en adoptant des stratégies et des plans de coopération nationaux en matière de SRI.

Deuxièmement, les autorités compétentes devraient coopérer au sein d'un réseau permettant une coordination sûre et efficace, un échange coordonné d'informations ainsi que la détection et l'intervention au niveau de l'UE. Au sein de ce réseau, les États membres devraient échanger des informations et coopérer pour faire face aux menaces et incidents relevant de la SRI conformément au plan européen de coopération en matière de SRI. Afin de garantir que toutes les autorités concernées participent de façon appropriée et en temps utile, la proposition exige également que les incidents s'apparentant à des infractions pénales soient signalés aux services répressifs et qu'Europol soit associé aux mécanismes de coordination à l'échelle de l'UE.

Troisièmement, la proposition vise, en s'inspirant de la directive-cadre sur les communications électroniques, à créer une culture de gestion des risques et à favoriser le

partage d'informations entre le secteur privé et le secteur public. Les entreprises de certains secteurs critiques ainsi que les administrations publiques seront tenues d'évaluer les risques qu'elles courent et d'adopter des mesures appropriées et proportionnées pour garantir la SRI. Ces entités seront tenues de signaler aux autorités compétentes tout incident qui compromet gravement leurs réseaux et systèmes d'information et a un impact significatif sur la continuité des services critiques et la fourniture des biens.

3. OBSERVATIONS SUR LA POSITION DU CONSEIL

Dans l'ensemble, la position du Conseil entérine le principal objectif de la proposition de la Commission, à savoir assurer un niveau élevé commun de sécurité des réseaux et systèmes d'information. Toutefois, le Conseil a introduit un certain nombre de changements quant à la façon d'atteindre cet objectif.

Moyens disponibles au niveau national en matière de cybersécurité

Aux termes de la position du Conseil, les États membres seront tenus d'adopter une stratégie nationale en matière de SRI définissant les objectifs stratégiques et les mesures politiques et réglementaires appropriées en matière de cybersécurité. Les États membres seront également tenus de désigner une autorité nationale compétente pour la mise en œuvre et le contrôle de l'application de la directive, ainsi que des «centres de réponse aux incidents de sécurité informatique» (CSIRT), chargés de la gestion des incidents et des risques.

Bien que la position du Conseil n'impose pas aux États membres d'adopter un plan national de coopération en matière de SRI comme l'envisageait la proposition initiale, cette position peut être soutenue car certains aspects du plan de coopération sont conservés dans les dispositions relatives à la stratégie nationale en matière de SRI.

Coopération entre les États membres

Aux termes de la position du Conseil, la directive instituera un «groupe de coopération» composé de représentants des États membres, de la Commission et de l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) et dont la mission sera de soutenir et de faciliter la coopération stratégique et l'échange d'informations entre les États membres. La directive instituera également un «réseau des centres de réponse aux incidents de sécurité informatique» («réseau des CSIRT») afin de promouvoir une coopération opérationnelle rapide et efficace sur des incidents concrets liés à la cybersécurité et le partage d'informations sur les risques.

Bien qu'elle suive une approche sensiblement différente de celle de la proposition initiale, la position du Conseil peut être soutenue car elle correspond globalement à l'objectif d'une amélioration de la coopération entre les États membres.

Exigences en matière de sécurité et de notification pour les opérateurs fournissant des services essentiels

Aux termes de la position du Conseil, les opérateurs de services essentiels (équivalant aux «opérateurs d'infrastructures critiques» de la proposition initiale) seront tenus d'adopter les mesures de sécurité appropriées et de notifier les incidents graves aux autorités nationales compétentes. Toutefois, le Conseil n'a pas fait sienne l'obligation pour les autorités nationales compétentes de notifier aux services répressifs les incidents s'apparentant à des infractions pénales.

À l'instar de la proposition initiale, la position du Conseil vise les opérateurs des secteurs suivants: énergie, transports, banques, infrastructures de marchés financiers et santé. Toutefois, elle inclut en outre les secteurs de l'eau et des infrastructures numériques.

Les États membres seront tenus d'identifier ces opérateurs sur la base de critères tels que le caractère essentiel du service pour le maintien d'activités sociétales ou économiques critiques. Bien que ce processus d'identification n'ait pas été prévu dans la proposition initiale, il peut être accepté compte tenu de l'obligation faite aux États membres de communiquer à la Commission les informations lui permettant de s'assurer qu'ils suivent des approches cohérentes dans l'identification des opérateurs de services essentiels.

Les administrations publiques ne sont pas expressément mentionnées dans la position du Conseil. Cependant, lorsqu'elles répondent aux critères énumérés à l'article 5, les États membres devront les considérer comme des opérateurs de services essentiels, puisque ces opérateurs peuvent aussi bien être des entités publiques que privées.

Exigences en matière de sécurité et de notification pour les fournisseurs de services numériques

Aux termes de la position du Conseil, les États membres devront s'assurer que les fournisseurs de services numériques prennent des mesures de sécurité appropriées et notifient les incidents à l'autorité compétente. La position du Conseil couvre les places de marché en ligne (équivalant aux «plateformes de commerce électronique» de la proposition initiale), les services d'informatique en nuage et les moteurs de recherche. Contrairement à la proposition modifiée, la position du Conseil n'inclut pas:

- les passerelles de paiement par internet – celles-ci sont désormais couvertes par la directive révisée sur les services de paiement;
- les magasins d'applications en ligne – qui sont censés relever des places de marché en ligne;
- les réseaux sociaux – conformément à l'accord politique entre le Conseil et le Parlement européen.

Aux termes de la position du Conseil, la Commission s'est vu conférer des compétences d'exécution pour fixer les modalités de procédure nécessaires au fonctionnement du groupe de coopération et clarifier certains éléments concernant les fournisseurs de services numériques, y compris les formats et les procédures que ces derniers doivent appliquer pour respecter les exigences en matière de notification.

La Commission approuve les conclusions qui précèdent.

À la suite des discussions tripartites informelles des 14 octobre 2014, 11 novembre 2014, 30 avril 2015, 29 juin 2015, 17 novembre 2015 et 7 décembre 2015, le Parlement et le Conseil sont parvenus à un accord politique provisoire sur le texte.

Cet accord politique a été confirmé par le Conseil le 18 décembre 2015. Le 17 mai 2016, le Conseil a arrêté sa position en première lecture.

4. CONCLUSION

La Commission approuve l'issue des négociations interinstitutionnelles et peut donc accepter la position adoptée par le Conseil en première lecture.