Informations de base

2013/0027(COD) COD - Procédure législative ordinaire (ex-procedure codécision) Directive	Procédure terminée
Niveau élevé commun de sécurité des réseaux et de l'information dans l'Union Abrogation 2020/0359(COD) **Subject** 2.80 Coopération et simplification administratives 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 7.30.09 Sécurité publique	

Acteurs principaux

Parlement européen

Commission au fond	Rapporteur(e)	Date de nomination
IMCO Marché intérieur et protection des consommateurs	SCHWAB Andreas (PPE)	20/03/2013
	Rapporteur(e) fictif/fictive DANTI Nicola (S&D) FORD Vicky (ECR) GUOGA Antanas (ALDE) ALBRECHT Jan Philipp (Verts/ALE)	

Commission à fond précédente	Rapporteur(e) précédent(e)	Date de nomination
IMCO Marché intérieur et protection des consommateurs	SCHWAB Andreas (PPE)	20/03/2013

Commission pour avis précédente	Rapporteur(e) pour avis précédent(e)	Date de nomination
AFET Affaires étrangères	GOMES Ana (S&D)	19/02/2013
INTA Commerce international	La commission a décidé de ne pas donner d'avis.	
BUDG Budgets	La commission a décidé de ne pas donner d'avis.	

ECON	Affaires économiques et monétaires	La commission a décidé de ne pas donner d'avis.	
ENVI	Environnement, climat et sécurité alimentaire	La commission a décidé de ne pas donner d'avis.	
ITRE	Industrie, recherche et énergie (Commission associée)	DEL CASTILLO VERA Pilar (PPE)	23/05/2013
TRAN	Transports et tourisme	La commission a décidé de ne pas donner d'avis.	
JURI	Affaires juridiques	La commission a décidé de ne pas donner d'avis.	
LIBE	Libertés civiles, justice et affaires intérieures (Commission associée)	SCHLYTER Carl (Verts/ALE)	07/03/2013

Conseil de l'Union européenne

Formation du Conseil	Réunions	Date
Compétitivité (marché intérieur, industrie, recherche et espace)	3451	2016-02-29
Transports, télécommunications et énergie	3243	2013-06-06
Transports, télécommunications et énergie	3278	2013-12-05
Transports, télécommunications et énergie	3318	2014-06-05

Commission européenne

DG de la Commission	Commissaire
Réseaux de communication, contenu et technologies	KROES Neelie

Comité économique et social européen

Evénements clés

Date	Evénement	Référence	Résumé
07/02/2013	Publication de la proposition législative	COM(2013)0048	Résumé
15/04/2013	Annonce en plénière de la saisine de la commission, 1ère lecture		
06/06/2013	Débat au Conseil		Résumé
12/09/2013	Annonce en plénière de la saisine des commissions associées		
05/12/2013	Débat au Conseil		Résumé
23/01/2014	Vote en commission,1ère lecture		
12/02/2014	Dépôt du rapport de la commission, 1ère lecture	A7-0103/2014	Résumé
12/03/2014	Débat en plénière	CRE link	
13/03/2014	Décision du Parlement, 1ère lecture	T7-0244/2014	Résumé

13/03/2014	Résultat du vote au parlement		
05/06/2014	Débat au Conseil		
06/10/2014	Ouverture des négociations interinstitutionnelles après 1ère lecture par la commission parlementaire		
14/01/2016	Approbation en commission du texte accordé aux négociations interinstitutionnelles en 2ème lecture	PE612.044 PE612.045	
17/05/2016	Publication de la position du Conseil	05581/1/2016	Résumé
09/06/2016	Annonce en plénière de la saisine de la commission, 2ème lecture		
14/06/2016	Vote en commission, 2ème lecture		
17/06/2016	Dépôt de la recommandation de la commission, 2ème lecture	A8-0211/2016	Résumé
05/07/2016	Débat en plénière	CRE link	
06/07/2016	Décision du Parlement, 1ère lecture	T8-0303/2016	Résumé
06/07/2016	Résultat du vote au parlement		
06/07/2016	Signature de l'acte final		
06/07/2016	Fin de la procédure au Parlement		
19/07/2016	Publication de l'acte final au Journal officiel		

Informations techniques

Référence de la procédure	2013/0027(COD)
Type de procédure	COD - Procédure législative ordinaire (ex-procedure codécision)
Sous-type de procédure	Législation
Instrument législatif	Directive
	Abrogation 2020/0359(COD)
Base juridique	Traité sur le fonctionnement de l'UE TFEU 114-p1
Autre base juridique	Règlement du Parlement EP 165
Consultation obligatoire d'autres institutions	Comité économique et social européen
État de la procédure	Procédure terminée
Dossier de la commission	IMCO/8/05266

Portail de documentation

Parlement Européen

Type de document	Commission	Référence	Date	Résumé
Projet de rapport de la commission		PE514.882	10/07/2013	
Amendements déposés en commission		PE519.524	30/09/2013	
Amendements déposés en commission		PE519.685	02/10/2013	
Amendements déposés en commission		PE523.040	19/11/2013	
Avis de la commission	AFET	PE516.830	05/12/2013	
Avis de la commission	ITRE	PE519.596	19/12/2013	
Amendements déposés en commission		PE521.696	09/01/2014	

Avis de la commission	LIBE	PE514.755	15/01/2014	
Rapport déposé de la commission, 1ère lecture/lecture unique		A7-0103/2014	12/02/2014	Résumé
Texte adopté du Parlement, 1ère lecture/lecture unique		T7-0244/2014	13/03/2014	Résumé
Projet de rapport de la commission		PE584.110	14/06/2016	
Recommandation déposée de la commission, 2e lecture		A8-0211/2016	17/06/2016	Résumé
Texte adopté du Parlement, 2ème lecture		T8-0303/2016	06/07/2016	Résumé
Texte convenu lors de négociations interinstitutionnelles		PE612.044	04/10/2017	
Lettre de la commission parlementaire confirmant l' accord interinstitutionnel		PE612.045	04/10/2017	

Conseil de l'Union

Type de document	Référence	Date	Résumé
Déclaration du Conseil sur sa position	08300/2016	29/04/2016	
Position du Conseil	05581/1/2016	17/05/2016	Résumé
Projet d'acte final	00026/2016/LEX	06/07/2016	

Commission Européenne

Type de document	Référence	Date	Résumé
Document annexé à la procédure	SWD(2013)0032	07/02/2013	
Document annexé à la procédure	SWD(2013)0031	07/02/2013	
Document de base législatif	COM(2013)0048	07/02/2013	Résumé
Réaction de la Commission sur le texte adopté en plénière	SP(2014)455	10/06/2014	
Communication de la Commission sur la position du Conseil	COM(2016)0363	30/05/2016	Résumé
Document de suivi	COM(2019)0546	28/10/2019	

Parlements nationaux

Type de document	Parlement /Chambre	Référence	Date	Résumé
Contribution	ES_PARLIAMENT	COM(2013)0048	19/03/2013	
Contribution	DE_BUNDESRAT	COM(2013)0048	01/04/2013	
Contribution	PT_PARLIAMENT	COM(2013)0048	10/04/2013	
Contribution	RO_SENATE	COM(2013)0048	19/04/2013	
Contribution	CZ_SENATE	COM(2013)0048	29/05/2013	

Autres Institutions et organes

Institution/organe	Type de document	Référence	Date	Résumé

ESC	Comité économique et social: avis, rapport	CES1414/2013	22/05/2013	
EDPS	Document annexé à la procédure	N7-0072/2014 JO C 032 04.02.2014, p. 0019	14/06/2013	Résumé
ECB	Banque centrale européenne: avis, orientation, rapport	CON/2014/0058 JO C 352 07.10.2014, p. 0004	25/07/2014	Résumé

Informations complémentaires

Source	Document	Date
Parlements nationaux	IPEX	
Commission européenne	EUR-Lex	

Acte final

Directive 2016/1148
JO L 194 19.07.2016, p. 0001 Résumé

Niveau élevé commun de sécurité des réseaux et de l'information dans l'Union

2013/0027(COD) - 07/02/2013 - Document de base législatif

OBJECTIF : assurer un niveau commun élevé de sécurité des réseaux et de l'information (SRI) dans l'Union.

ACTE PROPOSÉ : Directive du Parlement européen et du Conseil.

RÔLE DU PARLEMENT EUROPÉEN : le Parlement statue conformément à la procédure législative ordinaire sur un pied d'égalité avec le Conseil.

CONTEXTE : les réseaux et les systèmes informatiques jouent un rôle capital dans la circulation transfrontière des biens, des services et des personnes. Compte tenu de cette dimension transnationale, toute perturbation dans un État membre peut avoir une incidence sur d'autres États membres et sur l'UE dans son ensemble. **La fiabilité des réseaux et systèmes informatiques est donc essentielle au bon fonctionnement du marché intérieur.**

L'ampleur et la fréquence des incidents de sécurité, d'origine malveillante ou accidentelle, ne cessent de croître : 57% des personnes qui se sont exprimées dans le cadre d'une consultation publique lancée par la Commission, ont indiqué avoir été confrontées, pendant l'année écoulée, à des incidents liés à la cybersécurité ayant eu une incidence grave sur leurs activité. Un sondage Eurobaromètre de 2012 a révélé que 38% des internautes de l'UE étaient préoccupés par la sécurité des paiements en ligne.

Il n'existe actuellement aucun véritable cadre au niveau de l'UE dans lequel pourraient s'inscrire la coopération et la collaboration ainsi que le partage d'informations de confiance sur les risques et incidents de SRI entre les États membres. Or, la stratégie numérique pour l'Europe ainsi que les conclusions du Conseil la concernant soulignent bien que la confiance et la sécurité sont des conditions préalables fondamentales pour favoriser une adoption généralisée des technologies de l'information et de la communication.

La présente proposition est présentée en liaison avec la communication conjointe de la Commission et de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité concernant une **stratégie européenne en matière de cybersécurité**.

ANALYSE D'IMPACT : la Commission a analysé **trois options** différentes.

- ***Option 1*** : scénario du **statu quo**: maintien de l'approche actuelle.
- ***Option 2*** : **approche réglementaire** consistant en une proposition législative établissant un cadre juridique commun de l'UE en matière de SRI en ce qui concerne les moyens des États membres, les mécanismes de coopération au niveau de l'UE et les exigences applicables aux principaux acteurs privés et aux administrations publiques.
- ***Option 3*** : **approche mixte** combinant des initiatives basées sur la bonne volonté des États membres en ce qui concerne les moyens SRI et les mécanismes de coopération au niveau de l'UE avec des exigences réglementaires concernant les principaux acteurs privés et les administrations publiques.

La Commission a conclu que **l'option 2** serait celle qui aurait les effets positifs les plus prononcés. L'évaluation quantitative a montré que cette option n'imposerait pas une charge excessive aux États membres. Pour le secteur privé, les coûts seraient limités aussi car de nombreuses entités concernées sont déjà censées répondre à des exigences de sécurité existante.

BASE JURIDIQUE : article 114 du traité sur le fonctionnement de l'Union européenne (TFUE).

CONTENU : la proposition de directive vise à **revoir en profondeur la manière dont la SRI est abordée dans l'UE**. Elle prévoit d'imposer **des obligations réglementaires afin que les règles soient les mêmes partout** et que les lacunes législatives existantes puissent être comblées. Les objectifs de la directive proposée sont les suivants :

1°) exiger 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 SRI, en mettant sur pied **des équipes d'intervention** en cas d'urgence informatique (CERT) et en adoptant **des stratégies et des plans de coopération nationaux** en matière de SRI.

2°) prévoir que les autorités compétentes **coopèrent 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 échangeraient des informations et coopéreraient, avec le concours permanent de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) pour faire face aux menaces et incidents SRI et faciliter une application convergente de la directive dans toute l'UE.

3°) créer une culture de gestion des risques et **favoriser le partage d'informations entre le secteur privé et le secteur public**. Les entreprises des **secteurs critiques** - à savoir les secteurs de la banque, des bourses de valeurs, de la production, du transport et de la distribution d'énergie, des transports (aérien, ferroviaire, maritime), de la santé, des services internet - ainsi que les administrations publiques seraient tenues :

- **d'évaluer les risques** qu'elles courent et d'adopter des mesures appropriées et proportionnées pour garantir la SRI ;
- **de signaler aux autorités compétentes** tout incident de nature à compromettre sérieusement leurs réseaux et systèmes informatiques et ayant un impact significatif sur la continuité des services critiques et la fourniture des biens.

INCIDENCE BUDGÉTAIRE : la coopération et l'échange d'informations entre les États membres devraient se dérouler avec l'appui d'une **infrastructure sécurisée**. La proposition n'aura une incidence budgétaire pour l'UE que si les États membres décident d'adapter une infrastructure existante (telle que s-TESTA) et de confier les travaux de mise en œuvre à la Commission au titre du cadre financier pluriannuel 2014-2020. Le coût unique estimé serait de **1.250.000 EUR**, à condition que des fonds suffisants soient disponibles au titre du Mécanisme pour l'interconnexion en Europe (MIE).

Les États membres peuvent aussi décider soit de partager le coût unique lié à l'adaptation d'une infrastructure existante, soit de créer une nouvelle infrastructure et d'en supporter les coûts, qui sont estimés à environ **10 millions EUR par an**.

ACTES DÉLÉGUÉS : la proposition contient des dispositions habilitant la Commission à adopter des actes délégués conformément à l'article 290 du traité sur le fonctionnement de l'Union européenne.

Niveau élevé commun de sécurité des réseaux et de l'information dans l'Union

2013/0027(COD) - 06/06/2013

Sur la base d'un rapport concernant **l'état d'avancement des travaux** établi par la présidence irlandaise, le Conseil a examiné la proposition de directive visant à assurer un niveau commun élevé de sécurité des réseaux de communications électroniques et des systèmes d'information de l'UE. La présidence a identifié une série de questions qui, selon elles, souhaiteraient être discutées par les délégations :

Analyse d'impact (AI) : s'agissant de l'AI qui accompagne la proposition, un certain nombre d'États membres a fait remarquer qu'il semble y avoir certaines divergences entre les deux documents et que, en particulier, l'AI **n'a pas suffisamment justifié les raisons** pour lesquelles les prestataires de services de la société de l'information ont été inclus dans la proposition tandis que les fabricants de matériel ou de logiciels ont été exclus. Les États membres ont également souligné les faiblesses de l'AI en ce qui concerne l'impact de la proposition sur l'emploi, la compétitivité et l'innovation, la protection des données, les opérations des entreprises multinationales, le climat d'investissement, etc. La plupart des États membres ont également soulevé **la question de l'importante des coûts liés à la mise en œuvre** de la directive proposée et regretté que l'AI ne soit pas parvenue à évaluer correctement les avantages escomptés.

Sur un plan plus fondamental, les États membres souhaitent que la Commission fournisse **davantage d'explications sur les raisons qui l'on conduit à privilégier l'approche réglementaire par rapport à une approche volontaire** pour lutter contre le niveau inégal de capacités en matière de sécurité des réseaux dans l'UE et le partage insuffisant des informations sur les incidents, les risques et menaces, que la Commission perçoit comme étant les causes profondes de la situation actuelle. Les délégations ont demandé davantage d'informations sur les entreprises et autres parties prenantes qui ont répondu à la consultation publique lancée par la Commission, de façon à leur permettre de mieux évaluer les domaines où il existe des problèmes urgents.

Champ d'application : des discussions plus approfondies seront nécessaires sur la question de savoir quels «**acteurs du marché**» entreraient dans le champ d'application de la directive proposée. À cet égard, des doutes ont été exprimés quant à la proposition de soumettre les prestataires de services de la société de l'information aux mêmes obligations que les opérateurs d'infrastructures critiques et des questions ont été soulevées au sujet de la liste non exhaustive des acteurs du marché proposée.

Cadre organisationnel : en ce qui concerne le cadre organisationnel pour la mise en œuvre de la directive proposée, **les délégations n'ont pas encore exprimé des positions fermes** sur la structure de gouvernance proposée dans la mesure où ils mènent des consultations nationales avec les parties prenantes et analysent les détails de la proposition dans le contexte de cyberstratégies nationales existantes ou prévues.

Niveau élevé commun de sécurité des réseaux et de l'information dans l'Union

2013/0027(COD) - 12/02/2014 - Rapport déposé de la commission, 1ère lecture/lecture unique

La commission du marché intérieur et de la protection des consommateurs a adopté le rapport d'Andreas SCHWAB (PPE, DE) 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.

La commission de l'industrie, de la recherche et de l'énergie et la commission des libertés civiles, de la justice et des affaires intérieures, exerçant les prérogatives de commissions associées conformément à l'article 50 du règlement intérieur du Parlement, ont également été consultées pour émettre un avis sur le présent rapport.

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

Champ d'application : le projet de directive vise à imposer des obligations aux administrations publiques et aux acteurs du marché, y compris aux infrastructures critiques et aux services de la société de l'information.

Afin de veiller à la proportionnalité de l'application de la directive, les députés sont d'avis que les mesures obligatoires prévues au chapitre IV devraient être limitées aux infrastructures qui sont critiques au sens strict. Ils ont donc suggéré **de ne pas inclure les services de la société de l'information** à l'annexe II de la directive (liste des acteurs du marché).

En revanche, la directive devrait être **axée sur l'infrastructure critique essentielle au maintien des fonctions économiques et sociétales vitales** dans le domaine de l'énergie, des transports, des services bancaires, des infrastructures de marchés financiers ou des soins de santé. Les développeurs de logiciels et les fabricants de matériel devraient dès lors être exclus du champ d'application de la directive.

Protection et traitement des données à caractère personnel : les députés ont insisté pour que tout traitement de données à caractère personnel dans les États membres en vertu de la directive soit réalisé dans le respect de la directive 95/46/CE et de la directive 2002/58/CE. Toute utilisation des données personnelles devrait être limitée au strict nécessaire et ces données devraient être aussi anonymes que possible, voire totalement anonymes.

Autorités et guichets uniques compétents au niveau national en matière de sécurité des réseaux et systèmes informatiques : les députés ont proposé de modifier la directive afin d'autoriser la désignation de **plusieurs autorités compétentes** par État membre. Toutefois, afin de garantir une application cohérente dans l'État membre et de permettre une coopération efficace et simplifiée au niveau de l'Union, chaque État membre devrait désigner un **guichet unique**. Le guichet unique assurerait, entre autres, la coopération transfrontière avec d'autres guichets uniques.

Équipes d'intervention en cas d'urgence informatique (CERT) : chaque État membre devrait mettre en place **au moins une** équipe d'intervention en cas d'urgence informatique pour chacun des secteurs définis à l'annexe II, chargée de la gestion des incidents et des risques selon un processus bien défini.

Les CERT devraient disposer de moyens humains et financiers adéquats pour participer activement aux réseaux de coopération internationaux, et en particulier au niveau de l'Union.

Les CERT seraient encouragées à initier des exercices conjoints avec d'autres CERT, avec l'ensemble des CERT des États membres et avec les institutions compétentes des pays tiers, ainsi qu'avec les CERT des institutions multinationales et internationales, telles que l'OTAN et les Nations unies, et à y participer.

Réseau de coopération : en vue de renforcer les activités du réseau de coopération, les députés ont estimé que ce dernier devrait envisager **d'inviter les acteurs du marché et les fournisseurs de solutions en matière de cybersécurité** à y participer, si nécessaire. Par ailleurs, le réseau de coopération devrait publier un rapport annuel d'activités.

Exigences de sécurité et notification d'incidents : la proposition prévoit que la Commission est habilitée à adopter des actes délégués en ce qui concerne la définition des circonstances dans lesquelles les administrations publiques et les acteurs du marché sont tenus de notifier les incidents.

Afin de clarifier la portée des obligations et de les consacrer dans l'acte de base, il est proposé de **remplacer les actes délégués par des critères clairs** permettant de déterminer l'importance des incidents à notifier. Afin de déterminer l'ampleur de l'impact d'un incident, les critères suivants devraient être pris en compte : i) le nombre d'utilisateurs dont le service essentiel est concerné ; ii) la durée de l'incident ; iii) la portée géographique eu égard à la zone touchée par l'incident.

Après avoir consulté l'autorité compétente notifiée et l'acteur du marché concerné, le guichet unique pourrait **informer le public** de chaque incident lorsqu'il juge que la sensibilisation du public est nécessaire pour prévenir un incident ou gérer un incident en cours. Les États membres devraient encourager les acteurs du marché à divulguer les incidents affectant leur activité de leur plein gré dans leurs rapports financiers.

Mise en œuvre et exécution : la proposition prévoit que les acteurs du marché se soumettent à un audit exécuté par un organisme qualifié indépendant ou une autorité nationale et mettent les résultats de cet audit à la disposition de l'autorité compétente. Les députés ont préconisé pour leur part de **laisser une certaine flexibilité concernant la preuve de la conformité** avec les exigences imposées aux acteurs du marché en matière de sécurité, en admettant d'autres formes de preuve de la conformité que des audits de sécurité.

Les guichets uniques et les autorités chargées de la protection des données devraient mettre au point, en coopération avec l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), **des mécanismes d'échange d'informations et un formulaire unique** qui seraient utilisés pour les notifications d'incidents.

Sanctions : les députés ont proposé de préciser que lorsque les acteurs du marché ne respectent pas les obligations qui leur incombent en vertu de la directive, mais qu'ils n'ont pas agi de manière intentionnelle ou à la suite d'une négligence grave, aucune sanction ne soit imposée.

Niveau élevé commun de sécurité des réseaux et de l'information dans l'Union

2013/0027(COD) - 05/12/2013

Le Conseil a fait **le point des travaux** sur un projet de directive qui vise à assurer un niveau commun élevé de sécurité des réseaux de communication dans toute l'UE.

Les délégations reconnaissent qu'il faut prendre des mesures pour lutter contre les cyberattaques, mais **divergent quant au meilleur moyen d'assurer la sécurité des réseaux** dans toute l'UE :

- certaines délégations sont favorables à une **approche souple**, avec des règles contraignantes au niveau de l'UE limitées aux infrastructures critiques et aux exigences de base et complétées par des mesures facultatives et volontaires ;
- d'autres délégations ainsi que la Commission estiment que seules des **mesures juridiquement contraignantes** permettraient d'atteindre les niveaux de sécurité nécessaires à l'échelle de l'UE.

En ce qui concerne les **modalités pratiques**, de nouvelles discussions sont nécessaires sur plusieurs questions :

Stratégie et organisme compétent en matière de sécurité des réseaux (**SRI**) : toute perturbation importante survenant dans un État membre étant susceptible d'avoir des répercussions dans d'autres États membres, les délégations sont en mesure de soutenir le principe d'une entité de coordination au niveau national.

Toutefois, les États membres ayant déjà adopté des stratégies en matière de SRI portent un regard critique sur le chapitre II de la proposition, consacré aux **cadres nationaux des réseaux de l'information** : ces États souhaitent s'assurer que les exigences auxquelles les États membres devront satisfaire seront compatibles avec la pratique nationale en vigueur et n'iront pas au-delà.

Certaines délégations souhaitent obtenir des éclaircissements sur les termes «risques» ou «menaces» et se demandent à quoi correspondent exactement ces exigences et si elles devraient ne concerner que le secteur privé ou bien également le secteur public.

Autorité compétente et description de ses tâches : de nombreuses questions doivent encore être précisées, comme par exemple celle de savoir si l'autorité doit assumer des tâches opérationnelles, ce à quoi de nombreux États membres sont opposés, de même que la question de la répartition des responsabilités avec les équipes d'intervention en cas d'urgence informatique (CERT) nationales.

Gestion des risques et notification d'incidents : de nombreuses délégations ont demandé :

- si, outre les «opérateurs d'infrastructures critiques», la proposition devrait également couvrir les fournisseurs de services de la société de l'information ;
- que les États membres puissent déterminer avec plus de souplesse les secteurs qui constituent des infrastructures critiques nationales. Certaines délégations souhaitent limiter les exigences proposées au seul secteur privé ; d'autres demandent que les exigences relatives à la notification en cas d'atteinte à la sécurité soient volontaires ;
- dans quelle mesure les États membres pourraient en fait «garantir» que les parties sécurisent leurs réseaux et notifient les incidents.

Des préoccupations ont également été exprimées sur les conséquences que les notifications peuvent avoir sur la vie privée et la confidentialité de l'information.

Réseau de coopération : les discussions doivent se poursuivre sur les tâches du réseau de coopération, bien que de nombreuses délégations estiment qu'il ne devrait pas assumer de tâches opérationnelles.

Un certain nombre de questions demandent à être précisées, comme par exemple :

- qui présidera le réseau de coopération, quels en seront les coûts et quelles seront les relations et la répartition des responsabilités dans le cadre de la coopération entre les CERTS nationales, l'ENISA et Europol ;
- la question du partage d'informations au sein du réseau, que devrait selon certaines délégations, s'effectuer sur une base volontaire ;
- la nécessité du «système sécurisé d'échange d'informations» proposé et dédié ;
- le mécanisme d'alerte rapide proposé, notamment la question de savoir quelles informations seront échangées et à quel moment, et quelles seront les conséquences éventuelles pour l'incident ou le risque ;
- la question du moment et des conditions dans lesquelles une intervention coordonnée est nécessaire.

Selon la présidence, le principal défi consistera à convenir d'une approche assurant **un juste équilibre entre les règles contraignantes au niveau de l'UE et des mesures facultatives et volontaires**, qui devront toutes conduire à des niveaux similaires de préparation en matière de SRI entre les États membres et permettre à l'UE de répondre de manière efficace aux défis en matière de SRI.

Niveau élevé commun de sécurité des réseaux et de l'information dans l'Union

2013/0027(COD) - 13/03/2014 - Texte adopté du Parlement, 1ère lecture/lecture unique

Le Parlement européen a adopté par 521 voix pour, 22 contre et 25 abstentions, une résolution législative 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 (SRI) dans l'Union.

La position en première lecture adoptée par le Parlement européen suivant la procédure législative ordinaire a modifié la proposition de la Commission comme suit :

Champ d'application : le projet de directive vise à imposer des obligations aux administrations publiques et aux acteurs du marché, y compris aux infrastructures critiques et aux services de la société de l'information.

Afin de veiller à la proportionnalité de l'application de la directive, le Parlement est d'avis que les mesures obligatoires prévues au chapitre IV devraient être limitées aux infrastructures qui sont critiques au sens strict. Il a donc suggéré **de ne pas inclure les services de la société de l'information** (ex : passerelles de paiement par internet, réseaux sociaux, moteurs de recherche, services informatiques en nuage etc..) dans la liste des acteurs du marché figurant à l'annexe II de la directive.

En revanche, la directive devrait être **axée sur l'infrastructure critique essentielle au maintien des fonctions économiques et sociétales vitales** dans le domaine de l'énergie, des transports, des services bancaires, des infrastructures de marchés financiers ou des soins de santé. Les développeurs de logiciels et les fabricants de matériel devraient dès lors être exclus du champ d'application de la directive.

Protection et traitement des données à caractère personnel : les députés ont insisté pour que tout traitement de données à caractère personnel dans les États membres en vertu de la directive soit réalisé dans le respect de la directive 95/46/CE et de la directive 2002/58/CE. Toute utilisation des données personnelles devrait être limitée au strict nécessaire et ces données devraient être aussi anonymes que possible, voire totalement anonymes.

Stratégies nationales : le Parlement a proposé que les États membres puissent demander à **l'Agence européenne chargée de la sécurité des réseaux et de l'information** (ENISA) de les aider à élaborer leur stratégie nationale en matière de SRI et leurs plans nationaux de coopération en matière de SRI, à partir d'un modèle minimal commun de coopération en matière de SRI.

Autorités et guichets uniques compétents au niveau national en matière de sécurité des réseaux et systèmes informatiques : les députés ont proposé de modifier la directive afin d'autoriser la désignation de **plusieurs autorités compétentes** par État membre. Toutefois, afin de garantir une application cohérente dans l'État membre et de permettre une coopération efficace et simplifiée au niveau de l'Union, chaque État membre devrait désigner un **guichet unique**. Le guichet unique assurerait, entre autres, la coopération transfrontière avec d'autres guichets uniques.

Équipes d'intervention en cas d'urgence informatique (CERT) : chaque État membre devrait mettre en place **au moins une** équipe d'intervention en cas d'urgence informatique pour chacun des secteurs définis à l'annexe II, chargée de la gestion des incidents et des risques selon un processus bien défini.

Les CERT devraient disposer de moyens humains et financiers adéquats pour participer activement aux réseaux de coopération internationaux, et en particulier au niveau de l'Union.

Les CERT seraient encouragées à initier des exercices conjoints avec d'autres CERT, avec l'ensemble des CERT des États membres et avec les institutions compétentes des pays tiers, ainsi qu'avec les CERT des institutions multinationales et internationales, telles que l'OTAN et les Nations unies, et à y participer.

Réseau de coopération : en vue de renforcer les activités du réseau de coopération, les députés ont estimé que ce dernier devrait envisager **d'inviter les acteurs du marché et les fournisseurs de solutions en matière de cybersécurité** à y participer, si nécessaire. Par ailleurs, le réseau de coopération devrait publier un rapport annuel d'activités.

Les États membres auraient la possibilité de déterminer le **niveau de criticité des acteurs du marché** en tenant compte des spécificités des secteurs et de divers paramètres.

La Commission devrait adopter, au moyen d'actes délégués, un **ensemble de critères communs d'interconnexion et de sécurité** que doivent remplir les guichets uniques pour pouvoir échanger des informations sensibles et confidentielles au sein du réseau de coopération.

Exigences de sécurité et notification d'incidents : la proposition prévoit que la Commission est habilitée à adopter des actes délégués en ce qui concerne la définition des circonstances dans lesquelles les administrations publiques et les acteurs du marché sont tenus de notifier les incidents.

Afin de clarifier la portée des obligations et de les consacrer dans l'acte de base, il est proposé de **remplacer les actes délégués par des critères clairs** permettant de déterminer l'importance des incidents à notifier. Afin de déterminer l'ampleur de l'impact d'un incident, les critères suivants devraient être pris en compte : i) le nombre d'utilisateurs dont le service essentiel est concerné ; ii) la durée de l'incident ; iii) la portée géographique eu égard à la zone touchée par l'incident.

Après avoir consulté l'autorité compétente notifiée et l'acteur du marché concerné, le guichet unique pourrait **informer le public** de chaque incident lorsqu'il juge que la sensibilisation du public est nécessaire pour prévenir un incident ou gérer un incident en cours. Les États membres devraient encourager les acteurs du marché à divulguer les incidents affectant leur activité de leur plein gré dans leurs rapports financiers.

Mise en œuvre et exécution : la proposition prévoit que les acteurs du marché se soumettent à un audit exécuté par un organisme qualifié indépendant ou une autorité nationale et mettent les résultats de cet audit à la disposition de l'autorité compétente. Le Parlement a préconisé pour sa part de **laisser une certaine flexibilité concernant la preuve de la conformité** avec les exigences imposées aux acteurs du marché en matière de sécurité, en admettant d'autres formes de preuve de la conformité que des audits de sécurité.

Les guichets uniques et les autorités chargées de la protection des données devraient mettre au point, en coopération avec l'ENISA, **des mécanismes d'échange d'informations et un formulaire unique** qui seraient utilisés pour les notifications d'incidents.

Sanctions : les députés ont proposé de préciser que lorsque les acteurs du marché ne respectent pas les obligations qui leur incombent en vertu de la directive, mais qu'ils n'ont pas agi de manière intentionnelle ou à la suite d'une négligence grave, aucune sanction ne soit imposée.

Niveau élevé commun de sécurité des réseaux et de l'information dans l'Union

2013/0027(COD) - 14/06/2013 - Document annexé à la procédure

Avis du Contrôleur européen de la protection des données sur : i) la communication conjointe de la Commission et de la haute représentante de l'Union européenne pour les affaires étrangères et la politique de sécurité intitulée «Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé» et ii) sur la proposition de directive de la Commission concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union.

Le CEPD se félicite de la présentation d'une stratégie globale de cybersécurité et se réjouit du fait que la stratégie aille au-delà de l'approche traditionnelle consistant à opposer sécurité et respect de la vie privée en prévoyant une reconnaissance explicite du respect de la vie privée et de la protection des données en tant que valeurs essentielles.

Le CEPD constate toutefois que, du fait qu'elle ne prenne pas pleinement en considération d'autres initiatives parallèles de la Commission et d'autres procédures législatives en cours, comme la réforme de la protection des données et la proposition de règlement sur l'identification électronique et les services de confiance, la stratégie de cybersécurité **n'offre pas de vision véritablement complète et globale de la cybersécurité** au sein de l'Union et risque de perpétuer une approche fragmentée.

Le CEPD a formulé les recommandations suivantes :

Stratégie de cybersécurité :

- il serait judicieux de disposer d'une définition claire et restrictive de la «cybercriminalité» plutôt que d'une définition trop étendue ;

- la législation sur la protection des données devrait s'appliquer à toutes les actions de la stratégie, dès lors qu'elles concernent des mesures comprenant le traitement de données à caractère personnel ; c'est notamment le cas de nombreuses actions qui consistent en la mise en place de mécanismes de coopération ;
- en tant qu'organes de surveillance, les autorités chargées de la protection des données (APD) devraient dès être suffisamment associées à la mise en œuvre de mesures ayant trait au traitement de données à caractère personnel (comme le lancement du projet pilote de l'UE consacré à la lutte contre les réseaux zombies et les logiciels malveillants).

Directive sur la sécurité des réseaux et de l'information :

- introduire plus de clarté et de sécurité en dressant une liste exhaustive reprenant tous les acteurs du marché concernés, afin de garantir une approche pleinement harmonisée et intégrée de la sécurité au sein de l'UE;
- prévoir explicitement que la directive devrait s'appliquer sans préjudice des règles plus détaillées, existantes ou futures, dans des domaines spécifiques (comme celles qui seront définies concernant les fournisseurs de services de confiance dans la proposition de règlement sur l' identification électronique);
- ajouter un considérant pour expliquer la nécessité d'insérer la protection des données dès la conception et par défaut à un stade précoce de la conception des mécanismes établis dans la proposition ;
- préciser que le traitement des données à caractère personnel serait justifié dans la mesure où il est nécessaire pour atteindre les objectifs d' intérêt public poursuivis par la directive proposée ;
- définir les circonstances dans lesquelles une notification et préciser si la notification et ses documents justificatifs incluront ou non des détails sur les données à caractère personnel (comme les adresses IP) affectées par un incident de sécurité spécifique ;
- faire en sorte que l'exclusion des micro-entreprises du champ d'application de la notification ne s'applique pas aux acteurs qui jouent un rôle crucial dans la fourniture de services de la société de l'information, compte tenu notamment de la nature des informations qu'ils traitent (des données biométriques ou des données sensibles, par exemple);
- ajouter à la proposition des dispositions régissant l'échange ultérieur de données à caractère personnel par les autorités compétentes en matière de SRI avec d'autres destinataires, afin de garantir que les données ne soient divulguées qu'à des destinataires dont le traitement est nécessaire à l'accomplissement de leur mission ;
- définir le délai applicable à la conservation des données à caractère personnel;
- rappeler aux autorités compétentes leur obligation de fournir une information appropriée aux personnes concernées sur le traitement des données à caractère personnel, par exemple en publiant leur politique en matière de respect de la vie privée sur leur site web;
- ajouter une disposition relative au niveau de sécurité que les autorités compétentes en matière de SRI doivent respecter en ce qui concerne les informations collectées, traitées et échangées ;
- préciser que des critères relatifs à la participation des États membres au système sécurisé d'échange d'informations devraient assurer qu'un niveau élevé de sécurité soit garanti par tous les participants aux systèmes d'échange d'informations à toutes les étapes du traitement ;
- ajouter une description des rôles et responsabilités de la Commission et des États membres dans la création, l'exploitation et la maintenance du système sécurisé d'échange d'information ;
- préciser que tout transfert de données à caractère personnel vers des destinataires situés en dehors de l'UE doit être conforme à la directive 95/46/CE et au règlement (CE) n° 45/2001.

Niveau élevé commun de sécurité des réseaux et de l'information dans l'Union

2013/0027(COD) - 25/07/2014 - Banque centrale européenne: avis, orientation, rapport

AVIS DE LA BANQUE CENTRALE EUROPÉENNE (BCE) sur une 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 (SRI) dans l'Union.

N'ayant pas été consultée formellement par les législateurs, **la BCE a décidé d'émettre un avis, de sa propre initiative**, sur la directive proposée.

La BCE **soutient l'objectif de la directive** proposée de garantir un niveau commun élevé de SRI à travers l'Union et de parvenir à une cohérence d' approche en la matière dans tous les secteurs d'activité et tous les États membres.

Toutefois, la BCE considère que **la directive proposée ne doit pas porter préjudice au cadre existant en matière de surveillance des systèmes de paiement et de règlement de l'Eurosystème** qui comprend des dispositifs appropriés, notamment dans le domaine de la SRI. Pour cette raison, la BCE suggère de modifier la directive proposée de manière à refléter correctement les responsabilités de l'Eurosystème dans ce domaine.

La BCE note que les dispositifs existant en matière de surveillance en ce qui concerne les systèmes de paiement et les prestataires de services de paiement (PSP) prévoient déjà des procédures d'alerte précoces et des réactions coordonnées à l'intérieur et hors de l'Eurosystème pour traiter d' éventuelles menaces en matière de cybersécurité, semblables à celles définies dans la directive proposée.

Le SEBC a fixé des normes relatives aux obligations de déclaration et de gestion du risque pour les systèmes de paiement. De plus, la BCE évalue régulièrement les systèmes de règlement des opérations sur titres de manière à déterminer leur éligibilité aux opérations de crédit de l'Eurosystème.

Par conséquent, la BCE considère qu'il est nécessaire que les obligations figurant dans la directive proposée concernant les infrastructures de marché essentielles et leurs opérateurs **ne portent pas atteinte aux normes du règlement relatif aux obligations de surveillance des systèmes de paiement d'importance systémique (règlement SPIS), au cadre de politique de surveillance de l'Eurosystème ou à d'autres règlements de l' Union**, et en particulier le règlement européen des infrastructures de marché (EMIR) et à l'avenir le règlement portant sur l'amélioration du règlement des opérations sur titres dans l'Union européenne et sur les dépositaires centraux de titres (DCT).

De plus, ces obligations ne devraient pas interférer avec les missions de l'Autorité européenne des marchés financiers (AEMF) et de l'Autorité bancaire européenne (ABE), ni avec celles d'autres autorités de surveillance prudentielle.

Nonobstant ce qui précède, la BCE considère qu'il serait essentiel pour l'Eurosystème de partager les informations pertinentes avec le comité SRI à mettre en place conformément à l'article 19 de la directive proposée.

Niveau élevé commun de sécurité des réseaux et de l'information dans l'Union

2013/0027(COD) - 06/07/2016 - Texte adopté du Parlement, 2ème lecture

Le Parlement européen a adopté, en deuxième lecture de la procédure législative ordinaire, une résolution législative sur la position du Conseil en première lecture en vue de l'adoption de la 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.

Suivant la recommandation de sa commission du marché intérieur et de la protection des consommateurs, le Parlement a **adopté la position du Conseil en première** lecture sans y apporter d'amendements.

Pour rappel, la directive proposée vise à atteindre un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

Niveau élevé commun de sécurité des réseaux et de l'information dans l'Union

2013/0027(COD) - 30/05/2016 - Communication de la Commission sur la position du Conseil

La Commission a approuvé l'issue des négociations interinstitutionnelles et **a pu accepter la position adoptée par le Conseil en première lecture** 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.

La Commission a estimé que, dans l'ensemble, la position du Conseil **entérinait le principal objectif de la proposition de la Commission**, à savoir assurer un niveau élevé commun de sécurité des réseaux et systèmes d'information. Elle a toutefois noté que le Conseil avait introduit un certain nombre de changements quant à la façon d'atteindre cet objectif.

La Commission a formulé les observations suivantes :

Moyens disponibles au niveau national en matière de cybersécurité : aux termes de la position du Conseil, les États membres devraient : i) adopter une stratégie nationale en matière de SRI définissant les objectifs stratégiques en matière de cybersécurité ; ii) 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, **la Commission** soutient cette position 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 instituerait i) un «groupe de coopération» dont la mission serait de faciliter la coopération stratégique et l'échange d'informations entre les États membres ; ii) 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 Commission peut soutenir la position du Conseil 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 : la Commission note que 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 seraient 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, la Commission peut l'accepter 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.

Exigences en matière de sécurité et de notification pour les fournisseurs de services numériques : 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: i) **les passerelles de paiement par internet** - celles-ci sont désormais couvertes par la directive révisée sur les services de paiement; ii) **les magasins d'applications en ligne** - qui sont censés relever des places de marché en ligne; iii) **les réseaux sociaux** - conformément à l'accord politique entre le Conseil et le Parlement européen.

La Commission relève enfin qu'elle 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 procédures que ces derniers doivent appliquer pour respecter les exigences en matière de notification.

Niveau élevé commun de sécurité des réseaux et de l'information dans l'Union

2013/0027(COD) - 17/06/2016 - Recommandation déposée de la commission, 2e lecture

La commission du marché intérieur et de la protection des consommateurs a adopté la recommandation pour la deuxième lecture contenue dans le rapport le d'Andreas SCHWAB (PPE, DE) sur la position du Conseil en première lecture en vue de l'adoption de la 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.

La commission parlementaire a recommandé que le Parlement **adopte la position du Conseil en première lecture** sans y apporter d'amendements.

Pour rappel, la proposition de directive établit des mesures visant à assurer un niveau commun élevé de sécurité des réseaux et des systèmes d'information dans l'Union afin d'améliorer le fonctionnement du marché intérieur.

Niveau élevé commun de sécurité des réseaux et de l'information dans l'Union

2013/0027(COD) - 06/07/2016 - Acte final

OBJECTIF : assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

ACTE LÉGISLATIF : Directive (UE) 2016/1148 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.

CONTENU : la directive établit des mesures visant à **assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information (SRI) dans l'Union** afin d'améliorer le fonctionnement du marché intérieur.

Les réseaux et les services et systèmes d'information jouent un rôle crucial dans la société. Leur fiabilité et leur sécurité sont essentielles aux fonctions économiques et sociétales et notamment au fonctionnement du marché intérieur.

Or, les moyens existants ne sont pas suffisants pour assurer un niveau élevé de sécurité des réseaux et des systèmes d'information dans l'Union. Les niveaux de préparation sont très différents selon les États membres, ce qui se traduit par une fragmentation des approches dans l'Union.

Obligations relatives aux moyens disponibles au niveau national : la directive oblige les États membres à :

- adopter une **stratégie nationale** et à désigner **une autorité SRI nationale** disposant des ressources appropriées pour prévenir et gérer les risques et les incidents SRI et y apporter une réponse;
- mettre sur pied des **centres de réponse aux incidents de sécurité informatique** (CSIRT), chargés de la gestion des incidents et des risques.

Coopération : pour soutenir la coopération stratégique entre les États membres, renforcer la confiance et parvenir à un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, la directive prévoit l'institution d'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).

Ce groupe se verra confier des tâches telles que l'échange de meilleures pratiques et d'informations sur un certain nombre de questions ou l'examen des capacités et de l'état de préparation des États membres.

Afin de contribuer au renforcement de la confiance entre les États membres et de promouvoir une coopération opérationnelle rapide et effective, **un réseau des CSIRT nationaux** sera établi.

Exigences en matière de sécurité et de notification : la directive vise 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 auront l'obligation de signaler aux autorités compétentes tout incident qui compromet gravement leurs réseaux et systèmes d'information et qui a un impact significatif sur la continuité des services critiques et la fourniture des biens.

L'obligation de signalement des incidents de sécurité concerne :

- **les opérateurs de services essentiels** dans des secteurs tels que les services financiers, les transports, l'énergie et la santé;
- **les fournisseurs de services numériques** offrant trois types de services, à savoir : i) les places de marché en ligne, ii) les moteurs de recherche en ligne et iii) les services d'informatique en nuage
- **les administrations publiques** qui sont identifiées en tant qu'opérateurs de services essentiels.

Selon une **approche différentiée**, les exigences en matière de sécurité et de notification imposées aux fournisseurs de services numériques seront moins strictes que celles appliquées aux opérateurs de services essentiels.

ENTRÉE EN VIGUEUR : 8.8.2016.

TRANSPOSITION : au plus tard le 9.5.2018.

APPLICATION : à partir du 10.5.2016.

Niveau élevé commun de sécurité des réseaux et de l'information dans l'Union

2013/0027(COD) - 17/05/2016 - Position du Conseil

Le Conseil a adopté sa **position en première lecture** en vue de l'adoption de la 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.

La directive proposée établit des mesures visant à assurer un niveau commun élevé de sécurité des réseaux et des systèmes d'information dans l'Union afin d'améliorer le fonctionnement du marché intérieur.

Les principaux éléments de la position du Conseil portent sur les points suivants :

Obligations relatives aux moyens disponibles au niveau national en matière de cybersécurité : aux termes de la position du Conseil, les États membres seraient tenus :

- d'adopter une **stratégie nationale** définissant les objectifs stratégiques et les mesures politiques et réglementaires appropriées en vue de parvenir à un niveau élevé de sécurité des réseaux et des systèmes d'information et de le maintenir ;
- de **désigner une ou plusieurs autorités nationales compétentes** en matière de sécurité des réseaux et des systèmes d'information chargées de contrôler l'application de la directive au niveau national ;
- de **désigner un guichet unique national** en matière de sécurité des réseaux et des systèmes d'information exerçant une fonction de liaison pour assurer une coopération transfrontière entre les autorités des États membres, ainsi qu'avec les autorités pertinentes des autres États membres, le groupe de coopération et le réseau des centres de réponse aux incidents de sécurité informatiques (CSIRT). Le guichet unique fournirait également au groupe de coopération un rapport annuel concernant les notifications reçues ;
- de **désigner une ou plusieurs équipes de réactions aux incidents touchant la sécurité informatique dénommées «CSIRT»**, chargées de la gestion des incidents et des risques. Le texte prévoit dans son annexe I des obligations et des tâches incombant aux CSIRT.

Coopération : pour soutenir la coopération stratégique entre les États membres, renforcer la confiance et parvenir à un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, la position du Conseil prévoit :

- **l'institution d'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). Ce groupe se verrait confier des tâches spécifiques énumérées dans le texte, telles que l'échange de meilleures pratiques et d'informations sur un certain nombre de questions ou que l'examen des capacités et de l'état de préparation des États membres ;
- **la mise en place d'un réseau des CSIRT nationales** afin de contribuer au renforcement de la confiance entre les États membres et de promouvoir une coopération opérationnelle rapide et efficace. Le texte définit une liste de tâches imparties au réseau, telles que l'échange d'informations sur les services, les opérations et les capacités de coopération des CSIRT, le soutien aux États membres dans la gestion d'incidents transfrontières ou, dans certaines conditions, l'échange et l'évaluation d'informations liées à des incidents et aux risques correspondants.

Exigences en matière de sécurité et de notification : aux termes de la position du Conseil, la directive fixerait certaines obligations à deux types d'acteurs du marché, à savoir i) aux **opérateurs de services essentiels** et ii) aux **fournisseurs de services numériques**.

Selon une **approche différentiée**, les exigences en matière de sécurité et de notification imposées aux fournisseurs de services numériques seraient moins strictes que celles appliquées aux opérateurs de services essentiels.

Les deux types d'acteurs du marché seraient tenus de prendre des **mesures organisationnelles et techniques en vue de gérer les risques** qui menacent la sécurité des réseaux et systèmes d'information, ainsi qu'en vue de prévenir les incidents qui compromettent la sécurité de ces systèmes et d'en limiter l'impact. Par ailleurs, les incidents ayant un certain degré d'impact sur les services en question devraient être notifiés aux autorités nationales compétentes ou aux CSIRT.

Services essentiels (annexe II) : dans un certain nombre de secteurs importants d'un point de vue social et économique, dont ceux de l'énergie, des transports, de la banque, des infrastructures des marchés financiers, de la santé, de la fourniture et de la distribution d'eau potable et des infrastructures numériques, les États membres devraient identifier, sur la base de critères précis énoncés dans la directive, les opérateurs de services essentiels.

Services numériques (annexe III) : tous les fournisseurs de services numériques (à l'exception des micro et petites entreprises) offrant **trois types de services**, à savoir : i) les places de marché en ligne, ii) les moteurs de recherche en ligne et iii) les services d'informatique en nuage, devraient se conformer aux exigences de la directive.

Des entités qui n'ont pas été recensées en tant qu'opérateurs de services essentiels et qui ne sont pas des fournisseurs de services numériques pourraient notifier, à titre volontaire, certains incidents.

Transposition : les États membres devraient transposer la directive dans un délai de 21 mois à compter de sa date d'entrée en vigueur et disposeraient de 6 mois supplémentaires pour le recensement de leurs opérateurs fournissant des services essentiels.