# COM (2013) 48 final

**ASSEMBLÉE NATIONALE**

QUATORZIEME LÉGISLATURE

Reçu à la Présidence de l'Assemblée nationale
le 19 février 2013

**SÉNAT**

SESSION ORDINAIRE DE 2012-2013

Enregistré à la Présidence du Sénat
le 19 février 2013

## TEXTE SOUMIS EN APPLICATION DE L'ARTICLE 88-4 DE LA CONSTITUTION

PAR LE GOUVERNEMENT,

À L'ASSEMBLÉE NATIONALE ET AU SÉNAT.

**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

E 8076

**CONSEIL DE L'UNION EUROPÉENNE**

**Bruxelles, le 12 février 2013 (14.02)**
**(OR. en)**

**6342/13**

**Dossier interinstitutionnel: 2013/0027 (COD)**

**TELECOM 24**
**DATAPROTECT 14**
**CYBER 2**
**MI 104**
**CODEC 313**

**PROPOSITION**

| | |
|---|---|
| Origine: | Commission européenne |
| En date du: | 7 février 2013 |
| N° doc. Cion: | COM(2013) 48 final |
| Objet: | 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 |

Les délégations trouveront ci-joint la proposition de la Commission transmise par lettre de Monsieur Jordi AYET PUIGARNAU, Directeur, à Monsieur Uwe CORSEPIUS, Secrétaire général du Conseil de l'Union européenne.

_____

p.j.: COM(2013) 48 final

COMMISSION
EUROPÉENNE

Bruxelles, le 7.2.2013
COM(2013) 48 final

2013/0027 (COD)

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

{SWD(2013) 31 final}
{SWD(2013) 32 final}

# EXPOSÉ DES MOTIFS

La directive proposée vise à assurer un niveau commun élevé de sécurité des réseaux et de l'information (SRI). Aussi faut-il accroître la sécurité de l'internet et des réseaux et systèmes informatiques privés sur lesquels reposent les services dont dépend le fonctionnement de notre société et de nos économies. À cette fin, il est demandé aux États membres d'améliorer leur niveau de préparation et leur coopération mutuelle, et aux opérateurs d'infrastructures critiques telles que les réseaux d'énergie et de transports et aux principaux prestataires de services de la société de l'information (plateformes de commerce électronique, réseaux sociaux, etc.) ainsi qu'aux administrations publiques d'adopter les mesures appropriées pour gérer les risques de sécurité et signaler les incidents graves aux autorités nationales compétentes.

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. Celle-ci aura pour objectif de mettre en place un environnement numérique offrant des gages de sécurité et de confiance tout en garantissant la promotion et la défense des droits fondamentaux et autres valeurs essentielles de l'UE. La présente proposition est la principale mesure prévue par la stratégie. D'autres actions ayant trait à la sensibilisation, au développement d'un marché intérieur des produits et services de cybersécurité et à la promotion des investissements dans la R&D s'inscrivent également dans le cadre de cette stratégie. Elles seront complétées par d'autres mesures visant à intensifier la lutte contre la cybercriminalité et à doter l'UE d'une politique internationale en matière de cybersécurité.

## 1.1. Motivation et objectifs de la proposition

La sécurité des réseaux et de l'information revêt une importance de plus en plus grande pour l'économie et la société. Elle est aussi une condition préalable importante à la création d'un environnement fiable pour le commerce international des services. Or, les systèmes informatiques peuvent être touchés par des incidents de sécurité qui résultent d'erreurs humaines, de catastrophes naturelles, de défaillances techniques ou d'actes de malveillance. L'ampleur, la fréquence et la complexité de ces incidents ne cessent de croître. 57 % des personnes qui se sont exprimées dans le cadre de la consultation publique en ligne sur l'amélioration de la sécurité des réseaux et de l'information (SRI) dans l'UE[1], 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 activités. L'absence de SRI peut compromettre des services essentiels pour lesquels l'intégrité des réseaux et systèmes informatiques est capitale. Cela peut empêcher le fonctionnement des entreprises, entraîner des pertes financières considérables pour l'économie de l'UE et avoir une incidence négative sur le bien-être sociétal.

En outre, les systèmes d'information numériques, et notamment l'internet, sont des instruments de communication sans frontières interconnectés entre les États membres et ils revêtent une importance essentielle pour la circulation transfrontières des biens, des services et des personnes. 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 pour l'achèvement du

[1] La consultation publique en ligne organisée sur le thème «Améliorer la sécurité des réseaux et de l'information dans l'UE» s'est déroulée du 23 juillet au 15 octobre 2012.

marché unique du numérique et le fonctionnement harmonieux du marché intérieur. La survenue probable d'incidents, la fréquence de ces derniers et l'incapacité d'assurer une protection efficace sapent également la confiance du public à l'égard des réseaux et systèmes informatiques. Ainsi, un sondage Eurobaromètre de 2012 sur la cybersécurité a révélé que 38 % des internautes de l'UE étaient préoccupés par la sécurité des paiements en ligne et qu'ils avaient modifié leur comportement en raison d'inquiétudes liées à la sécurité: 18 % sont moins susceptibles de faire des achats en ligne et 15 % sont moins susceptibles d'utiliser les services bancaires en ligne[2].

La situation actuelle dans l'UE est le reflet de l'approche strictement volontaire suivie jusqu'à maintenant et ne fournit pas de protection suffisante contre les incidents et risques en matière de SRI dans l'ensemble de l'UE. Les moyens et mécanismes de SRI existants ne sont tout simplement pas suffisants pour suivre l'évolution rapide des changements sur le front des menaces et pour garantir un niveau commun élevé de protection dans tous les États membres.

En dépit des initiatives prises, les moyens disponibles et les niveaux de préparation sont très différents selon les États membres, ce qui se traduit par une fragmentation des approches dans l'UE. Étant donné que les réseaux et systèmes informatiques sont interconnectés, c'est l'ensemble de la SRI de l'UE qui peut être affaiblie par les États membres dont le niveau de protection est insuffisant. Cette situation nuit à la création d'un climat de confiance entre pairs, lequel est une condition préalable à la coopération et au partage d'informations. De ce fait, seule une minorité d'États membres disposant de moyens significatifs a établi une coopération.

Par conséquent, 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. Dans ce contexte, on risque de voir se multiplier les actions réglementaires non coordonnées, les stratégies incohérentes et les normes divergentes, et le niveau de protection contre les risques de SRI dans l'UE deviendrait alors insuffisant. On pourrait aussi voir apparaître des obstacles au sein du marché intérieur, qui occasionneraient des coûts de mise en conformité pour les entreprises qui exercent leurs activités dans plusieurs États membres.

En dernier lieu, les acteurs qui gèrent des infrastructures critiques ou qui fournissent des services essentiels au fonctionnement de la société ne sont pas soumis à des obligations appropriées en ce qui concerne l'adoption de mesures de gestion des risques et l'échange d'informations avec les autorités compétentes. Par conséquent, d'une part, faute d'incitations efficaces, les entreprises ne mettent pas en place de politique sérieuse de gestion des risques prévoyant notamment une évaluation des risques et l'adoption de mesures appropriées pour garantir la SRI et, d'autre part, une large proportion d'incidents n'est pas signalée aux autorités compétentes et passe inaperçue. Or, il est essentiel que les pouvoirs publics soient informés des incidents pour qu'ils puissent réagir, prendre les mesures d'atténuation nécessaires et fixer des priorités stratégiques adéquates en matière de SRI.

En vertu du cadre réglementaire actuellement en vigueur, seules les entreprises de télécommunications sont tenues d'adopter des mesures de gestion des risques et de signaler les incidents graves en matière de SRI. Pourtant, de nombreux autres secteurs fondent leurs activités sur les outils informatiques et la SRI devrait donc aussi faire partie de leurs préoccupations. Un certain nombre de fournisseurs d'infrastructures et de services spécifiques

[2] Eurobaromètre 390/2012.

sont particulièrement vulnérables car ils dépendant étroitement du bon fonctionnement des réseaux et systèmes informatiques. Ces secteurs jouent un rôle majeur dans la fourniture de services de support essentiels à notre économie et à notre société et la sécurité de leurs systèmes revêt une importance particulière pour le fonctionnement du marché intérieur. Il s'agit notamment des 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 et des administrations publiques.

Il faut donc revoir en profondeur la manière dont la SRI est abordée dans l'UE. Il est impératif d'imposer des obligations réglementaires afin que les règles soient les mêmes partout et que les lacunes législatives existantes puissent être comblées. Pour régler ces problèmes et relever le niveau de SRI dans l'Union européenne, les objectifs de la directive proposée sont les suivants.

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 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.

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 échangeraient des informations et coopéreraient pour faire face aux menaces et incidents SRI conformément au plan européen de coopération en matière de SRI.

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 des secteurs critiques cités ci-avant 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 sérieusement leurs réseaux et systèmes informatiques et a un impact significatif sur la continuité des services critiques et la fourniture des biens.

### 1.2. Contexte général

Dès 2001, dans sa communication sur la «Sécurité des réseaux et de l'information: proposition pour une approche politique européenne», la Commission soulignait l'importance croissante de la SRI[3].Elle a ensuite adopté, en 2006, «Une stratégie pour une société de l'information sûre»[4], qui visait à mettre en place une culture de SRI en Europe. Ses principaux éléments ont été approuvés par une résolution du Conseil[5].

La Commission a en outre adopté, le 30 mars 2009, une communication sur la protection des infrastructures d'information critiques (PIIC)[6] axée sur l'amélioration de la sécurité pour protéger l'Europe des perturbations informatiques. La communication prévoyait le lancement

[3] COM(2001) 298.
[4] COM (2006) 251 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0251:FIN:FR:PDF
[5] 2007/068/01.
[6] COM (2009) 149.

d'un plan d'action destiné à soutenir les efforts déployés par les États membres en matière de prévention et d'intervention. Ce plan a été approuvé par les conclusions de la présidence de la conférence ministérielle sur la protection des infrastructures d'information critiques, qui s'est tenue à Tallinn en 2009. Le 18 décembre 2009, le Conseil a adopté une résolution sur une approche européenne concertée en matière de sécurité des réseaux et de l'information[7].

La stratégie numérique pour l'Europe[8], adoptée en mai 2010, ainsi que les conclusions du Conseil la concernant[9] soulignent bien que la confiance et la sécurité sont des conditions préalables fondamentales pour favoriser une adoption généralisée des TIC et, partant, la réalisation des objectifs de la stratégie Europe 2020 en ce qui concerne la «croissance intelligente»[10]. Dans le chapitre de la stratégie numérique consacré à la confiance et à la sécurité, toutes les parties prenantes sont appelées à unir leurs forces dans un effort global pour renforcer la sécurité et la résilience des infrastructures TIC, en centrant leur action sur la prévention, la préparation et la sensibilisation, et à mettre en place des mécanismes efficaces et coordonnés en matière de sécurité. L'action-clé n° 6 de la stratégie numérique, en particulier, préconise l'adoption de mesures ayant pour but une politique renforcée et de haut niveau en matière de SRI.

Dans sa communication relative à la protection des infrastructures d'information critiques (PIIC) de mars 2011 intitulée «Réalisations et prochaines étapes: vers une cybersécurité mondiale»[11], la Commission a dressé un bilan des résultats obtenus depuis l'adoption du plan d'action PIIC en 2009. Elle a conclu que la mise en œuvre de ce plan montrait qu'il ne suffit pas d'appliquer des approches strictement nationales ou régionales pour s'attaquer aux problèmes de sécurité et de résilience et que l'Europe doit persévérer dans ses efforts visant à mettre en place une approche cohérente et coopérative dans l'ensemble de l'UE. Un certain nombre d'actions étaient annoncées dans la communication PIIC de 2011, dans laquelle la Commission enjoignait notamment aux États membres de se doter de moyens et d'un mécanisme de coopération transfrontières dans le domaine de la SRI. La plupart de ces actions auraient dû être menées à bien avant la fin 2012, mais elles n'ont pas encore été mises en œuvre.

Dans ses conclusions du 27 mai 2011 sur la PIIC, le Conseil de l'Union européenne a souligné la nécessité de garantir la sécurité et la résilience de nos systèmes et réseaux informatiques pour qu'ils résistent à toutes les perturbations possibles, qu'elles soient accidentelles ou intentionnelles, de favoriser un état de préparation, des mesures de sécurité et une capacité de résilience d'un niveau élevé dans toute l'Union européenne, d'améliorer les compétences techniques pour permettre à l'Europe de faire face aux problèmes de protection des réseaux et infrastructures informatiques et d'encourager la coopération entre les États membres en mettant en place des mécanismes de coopération entre les États membres en cas d'incident informatique.

### 1.3. Les dispositions européennes et internationales en vigueur dans ce domaine

En vertu du règlement (CE) n° 460/2004, la Communauté européenne a créé, en 2004, l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)[12], afin

---

7 2009/C 321/01.
8 COM(2010) 245.
9 Conclusions du Conseil du 31 mai 2010 concernant la stratégie numérique pour l'Europe (10130/10).
10 COM (2010) 2020 et conclusions du Conseil européen des 25 et 26 mars 2010 (EUCO 7/10).
11 COM(2011) 163.
12 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:FR:HTML

d'assurer un niveau élevé et efficace de SRI dans l'UE et de favoriser l'émergence d'une culture dans ce domaine. Une proposition de la Commission relative à la modernisation de l'ENISA a été adoptée le 30 septembre 2010[13] et est actuellement examinée par le Conseil et le Parlement européen. Le nouveau cadre pour les infrastructures de communications électroniques[14], en vigueur depuis novembre 2009, impose des obligations en matière de sécurité aux fournisseurs de communications électroniques[15]. Ces obligations devaient être transposées dans les législations nationales avant mai 2011.

Tous les acteurs qui sont responsables du traitement de données (p. ex. une banque ou un hôpital) sont obligés par le cadre réglementaire en matière de protection des données[16] d'instaurer des mesures de sécurité destinées à protéger les données à caractère personnel. En vertu de la proposition de la Commission relative à un règlement général sur la protection des données[17] de 2012, les responsables du traitement de données devraient notifier les violations de données à caractère personnel aux autorités nationales compétentes. Cela signifie, par exemple, qu'une atteinte à la SRI qui a une incidence sur la fourniture d'un service mais ne compromet pas de données à caractère personnel (une panne informatique dans une entreprise d'électricité entraînant une coupure totale d'électricité, par exemple) n'aurait pas à être signalée.

Le programme européen de protection des infrastructures critiques (EPCIP)[18], qui s'inscrit dans le cadre de la directive 2008/114/CE concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection, expose l'approche globale pour la protection générale des infrastructures critiques dans l'UE. Les objectifs de l'EPCIP sont parfaitement compatibles avec la présente proposition et la directive proposée devrait s'appliquer sans préjudice des dispositions de la directive 2008/114. L'EPCIP n'oblige pas les opérateurs à signaler les atteintes significatives à la sécurité et n'instaure pas de mécanisme de coopération et d'intervention des États membres en cas d'incident.

Les colégislateurs examinent actuellement la proposition de directive, soumise par la Commission, relative aux attaques visant les systèmes d'information[19], qui vise à harmoniser la pénalisation de certains actes. Elle ne couvre que la pénalisation d'actes précis mais n'aborde pas la prévention des risques et incidents de SRI, l'intervention en cas d'incidents de SRI ni l'atténuation de leurs conséquences. La directive proposée devrait s'appliquer sans préjudice des dispositions de la directive relative aux attaques visant les systèmes d'information.

Le 28 mars 2012, la Commission a adopté une communicationrelative à l'établissement d'un Centre européen de lutte contre la cybercriminalité[20]. Ce Centre, créé le 11 janvier 2013, fait partie d'Europol et sert de point focal dans la lutte contre la cybercriminalité au sein de l'UE. Il aura pour mission de mettre en commun le savoir-faire en matière de cybercriminalité au

---

13 COM(2010) 521.

14 See http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf.

15 Articles 13 *bis* et 13 *ter* de la directive «cadre».

16 Directive 2002/58/CE du 12 juillet 2002.

17 COM(2012) 11.

18 COM(2006) 786 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:FR:PDF.

19 COM (2010) 517 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:FR:PDF).

20 COM (2012) 140 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:FR:PDF).

niveau européen pour aider les États membres à se doter de moyens, de contribuer aux enquêtes cybercriminelles des États membres et de permettre, en étroite collaboration avec Eurojust, aux enquêteurs européens sur la cybercriminalité, relevant de la justice comme des services de répression, de s'exprimer d'une seule voix.

Les institutions, agences et organismes de l'Union ont créé leur propre équipe d'intervention en cas d'urgence informatique (CERT-EU).

Au niveau international, l'action de l'UE en matière de cybersécurité est à la fois bilatérale et multilatérale. Un groupe de travail UE-USA sur la cybersécurité et la cybercriminalité a été créé lors du sommet UE-USA de novembre 2010[21]. L'UE est également active dans les enceintes multilatérales concernées, telles que l'Organisation de coopération et de développement économiques (OCDE), l'Assemblée générale des Nations unies, l'Union internationale des télécommunications (UIT), l'organisation pour la sécurité et la coopération en Europe (OSCE), le sommet mondial sur la société de l'information et le forum de gouvernance de l'internet.

## 2. RÉSULTATS DES CONSULTATIONS DES PARTIES INTÉRESSÉES ET DES ANALYSES D'IMPACT

### 2.1. Consultation des parties intéressées et utilisation des compétences

Une consultation publique en ligne sur le thème «Accroître la SRI dans l'UE» s'est déroulée du 23 juillet au 15 octobre 2012. La Commission a reçu 160 réponses au questionnaire en ligne.

Ces réponses ont, avant tout, montré que les participants reconnaissaient, dans leur grande majorité, la nécessité d'accroître la SRI dans l'UE. On notera en particulier ce qui suit. 82,8 % des participants ont estimé que les pouvoirs publics de l'UE devraient prendre des mesures supplémentaires pour garantir un niveau élevé de SRI et que les utilisateurs des systèmes et des informations n'étaient pas conscients des menaces et incidents liés à la SRI, 66,3 % seraient en principe favorables à l'introduction d'exigences réglementaires pour gérer les risques de NRI et 84,8 % des participants ont estimé que ces exigences devraient être fixées au niveau de l'UE. Une forte proportion de participants était d'avis qu'il serait particulièrement important d'adopter des exigences en matière de SRI dans les domaines suivants: les secteurs bancaire et financier (91,1 %), l'énergie (89,4 %), les transports (81,7 %), la santé (89,4 %), les services internet (89,1 %), et les administrations publiques (87,5 %). Ils étaient 65,1 % à considérer que, si une obligation de signaler les incidents en matière de SRI aux autorités nationales compétentes devait être introduite, elle devrait être fixée au niveau de l'UE et ont souligné, pour 93,5 % d'entre eux, que les administrations devraient aussi y être soumises. Enfin, 63,4 % des participants ont déclaré qu'une obligation d'instaurer un mécanisme de gestion des risques de SRI à la pointe de la technologie ne représenterait pas de coûts supplémentaires significatifs pour eux et 72,3 % d'entre eux ont jugé que l'introduction d'une obligation de signaler les incidents en matière de SRI n'entraînerait pas non plus de coûts supplémentaires significatifs.

Les États membres ont été consultés dans le cadre de différentes formations du Conseil pertinentes, dans celui du Forum européen des États membres (EFMS), lors de la conférence de l'UE sur la cybersécurité organisée le 6 juillet 2012 par la Commission et le Service

[21] http://europa.eu/rapid/press-release_MEMO-10-597_fr.htm

européen pour l'action extérieure, et lors de réunions bilatérales *ad hoc* organisées à la demande de différents États membres.

Des discussions avec des entreprises du secteur privé ont également eu lieu dans le cadre du Partenariat public-privé européen pour la résilience[22] et dans des réunions bilatérales. En ce qui concerne le secteur public, des discussions ont eu lieu entre la Commission et l'ENISA et l'équipe CERT pour les institutions de l'UE.

## 2.2. Analyse d'impact

La Commission a réalisé une analyse d'impact de 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 car elle permettrait d'améliorer considérablement la protection des particuliers, entreprises et administrations de l'UE contre les incidents de SRI. En particulier, les obligations imposées aux États membres garantiraient un niveau approprié de préparation au niveau national et contribueraient à l'instauration d'un climat de confiance mutuelle, qui constitue une condition préalable à la mise en place d'une coopération efficace au niveau de l'UE. La création de mécanismes de coopération au niveau de l'UE par l'intermédiaire du réseau garantirait la cohérence et la coordination de la prévention et de l'intervention en cas de risques et d'incidents de SRI. Les exigences imposées aux administrations publiques et principaux acteurs privés en matière de gestion des risques de SRI constitueraient une forte incitation à gérer efficacement les risques liés à la sécurité. L'obligation de signaler les incidents de SRI ayant un impact significatif améliorerait la capacité d'intervention en cas d'incident et favoriserait la transparence. En outre, en mettant de l'ordre chez elle, l'UE pourrait davantage s'imposer sur la scène internationale et apparaître comme un partenaire encore plus crédible en matière de coopération au niveau bilatéral et multilatéral. Elle serait donc aussi mieux placée pour promouvoir à l'étranger les droits fondamentaux et les valeurs essentielles de l'UE.

L'évaluation quantitative a montré que l'option 2 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 existantes (par exemple l'obligation, pour les responsables du traitement de données, de prendre les mesures techniques et organisationnelles appropriées, y compris en matière de SRI, pour protéger les données à caractère personnel). Les dépenses actuellement consacrées à la sécurité dans le secteur privé ont également été prises en considération.

[22] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r.

La présente proposition respecte les principes reconnus par la Charte des droits fondamentaux de l'Union européenne et notamment le droit au respect de la vie privée et des communications, le droit à la protection des données à caractère personnel, la liberté d'entreprise, le droit de propriété ainsi que le droit à un recours effectif et à un procès équitable. La directive doit être mise en œuvre conformément à ces droits et principes.

## 3. ÉLÉMENTS JURIDIQUES DE LA PROPOSITION

### 3.1. Base juridique

L'Union européenne est habilitée à adopter des mesures destinées à établir ou assurer le fonctionnement du marché intérieur, conformément aux dispositions pertinentes des traités (article 26 du traité sur le fonctionnement de l'Union européenne – TFUE). En application de l'article 114 du TFUE, l'UE peut adopter des «mesures relatives au *rapprochement des dispositions législatives, réglementaires et administratives des États membres* qui ont pour objet l'établissement et le fonctionnement du marché intérieur».

Les réseaux et les systèmes informatiques jouent un rôle capital dans la circulation transfrontière des biens, des services et des personnes. Ils sont souvent interconnectés, et l'internet a, par nature, une dimension planétaire. Compte tenu de cette dimension transnationale intrinsèque, toute perturbation 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.

Le législateur européen a déjà reconnu la nécessité d'harmoniser les règles en matière de SRI pour permettre la mise en place du marché intérieur. C'est notamment l'objectif du règlement (CE) n° 460/2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)[23], qui est fondé sur l'article 114 du TFUE.

Les différences résultant de la disparité, entre les États membres, des moyens disponibles au niveau national, des politiques et du niveau de protection dans le domaine de la SRI ont créé à des entraves au marché intérieur et justifient une action de l'UE.

### 3.2. Subsidiarité

L'action de l'UE en matière de SRI se justifie par le principe de subsidiarité.

Premièrement, compte tenu de la dimension transnationale de la SRI, l'absence d'intervention au niveau de l'UE mènerait à une situation dans laquelle chaque État membre agirait seul, sans égard pour l'interdépendance des systèmes et réseaux informatiques. Introduire un degré approprié de coordination entre les États membres permettrait d'assurer une bonne gestion des risques de SRI dans le contexte transnational qui est le leur. Les disparités dans les réglementations relatives à la SRI constituent un obstacle pour les entreprises qui désirent exercer leurs activités dans différents pays, ainsi que pour la réalisation d'économies d'échelle au niveau mondial.

[23] Règlement (CE) n° 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information (JO L 077 du 13.3.2004, p. 1).

Deuxièmement, il est impératif d'imposer des obligations réglementaires au niveau de l'UE afin que les règles soient les mêmes partout et que les lacunes législatives puissent être comblées. Du fait de l'approche strictement volontaire suivie jusqu'à présent, seule une minorité d'États membres disposant de moyens significatifs a établi une coopération. Afin de garantir que la coopération englobe l'intégralité des États membres, il faut s'assurer qu'ils disposent tous du niveau minimum de moyens requis. Les mesures en matière de SRI adoptées par les gouvernements doivent être cohérentes et coordonnées afin de circonscrire les incidents de SRI et d'en limiter les conséquences. Au sein du réseau, les autorités compétentes et la Commission coopéreront, par l'échange de meilleures pratiques et avec le concours permanent de l'ENISA, pour faciliter une application convergente de la directive dans toute l'UE. En outre, des actions politiques concertées en matière de SRI peuvent avoir un fort impact positif sur la protection effective des droits fondamentaux et, en particulier, sur le droit à la protection des données à caractère personnel et de la vie privée. Une intervention au niveau de l'UE permettrait par conséquent d'accroître l'efficacité des politiques nationales existantes et de faciliter leur développement.

Les mesures proposées se justifient aussi en termes de proportionnalité. Les exigences imposées aux États membres correspondent à ce qui est strictement nécessaire pour atteindre le niveau approprié de préparation et permettre la coopération sur la base de la confiance. Ainsi, les États membres ont la faculté de tenir dûment compte des particularités nationales et les principes communs de l'UE peuvent être appliqués de manière proportionnée. L'étendue du champ d'application permet aux États membres d'appliquer la directive en fonction des risques réels encourus au niveau national et recensés dans la stratégie nationale en matière de SRI. Les exigences en matière de gestion des risques visent uniquement les entités critiques et imposent des mesures qui sont proportionnées aux risques. La consultation publique a montré à quel point la sécurité de ces entités critiques est importante. Les exigences relatives à la notification d'incidents ne concerneraient que les incidents ayant un impact significatif. Comme indiqué ci-dessus, ces mesures n'impliqueraient pas de coûts disproportionnés, car bon nombre de ces entités, en tant que responsables du traitement de données, sont déjà soumises par la réglementation en vigueur en matière de protection des données à l'obligation d'assurer la protection des données à caractère personnel.

Pour éviter que la charge imposée aux opérateurs de petite taille, et notamment aux PME, ne soit disproportionnée, les exigences devraient être proportionnées aux risques que présente le réseau ou le système informatique concerné et ne devraient pas être applicables aux micro-entreprises. Les risques devront d'abord être recensés par les entités soumises à ces obligations, qui devront décider des mesures à adopter pour les atténuer.

Les objectifs énoncés peuvent être mieux atteints par l'action envisagée au niveau de l'UE que par des actions engagées au niveau des États membres, compte tenu de la dimension transnationale des incidents et risques de SRI. L'Union européenne peut donc adopter des mesures conformément au principe de subsidiarité énoncé à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité, la directive proposée n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

Aux fins de la réalisation des objectifs, la Commission devrait se voir conférer le pouvoir d’adopter des actes délégués conformément à l’article 290 du traité sur le fonctionnement de l’Union européenne, afin de compléter ou de modifier certains éléments non essentiels de l’acte de base. La proposition de la Commission s'efforce également de favoriser une certaine proportionnalité dans la mise en œuvre des obligations imposées aux opérateurs publics et privés.

Afin de garantir des conditions uniformes d'application de l'acte de base, il convient que la Commission ait le pouvoir d’adopter des actes d’exécution conformément à l’article 291 du TFUE.

Compte tenu, notamment, de l'étendue du champ d'application de la directive proposée, du fait qu'elle concerne des domaines fortement réglementés et des obligations juridiques qui découlent de son chapitre IV, il convient que des documents explicatifs accompagnent la notification des mesures de transposition. Conformément à la déclaration politique commune des États membres et de la Commission du 28 septembre 2011 sur les documents explicatifs, les États membres se sont engagés à joindre à la notification de leurs mesures de transposition, dans les cas où cela se justifie, un ou plusieurs documents expliquant le lien entre les éléments d’une directive et les parties correspondantes des instruments nationaux de transposition. En ce qui concerne la présente directive, le législateur considère que la transmission de ces documents se justifie,

## 4. 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 à 1 250 000 EUR, serait imputé à la ligne budgétaire 09.03.02 du budget de l'UE – Réseaux de télécommunications (favoriser l'interconnexion et l'interopérabilité des services publics nationaux en ligne ainsi que l'accès à ces réseaux, chapitre 09.03, mécanisme pour l'interconnexion en Europe - réseaux de télécommunications) à condition que des fonds suffisants soient disponibles au titre du 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 d'EUR par an.

2013/0027 (COD)

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**

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 114,

vu la proposition de la Commission européenne,

après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen[1],

après consultation du contrôleur européen de la protection des données,

statuant conformément à la procédure législative ordinaire,

considérant ce qui suit:

(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.

(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.

(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.

(4) Il convient d'établir, au niveau de l'UE, un mécanisme de coopération qui permette l'échange d'informations et garantisse la coordination de la prévention et de l'intervention en ce qui concerne la sécurité des réseaux et de l'information («SRI»).

[1] JO C […] du […], p. […].

Pour que ce mécanisme soit efficace et ouvert à tous, il est essentiel que tous les États membres soient dotés d'un minimum de moyens et d'une stratégie garantissant un niveau élevé de SRI sur leur territoire. Les administrations publiques et les opérateurs d'infrastructures d'information critiques devraient par ailleurs être soumis à des exigences minimales en matière de sécurité, afin de promouvoir une culture de gestion des risques et de faire en sorte que les incidents les plus graves soient signalés.

(5) Pour que tous les incidents et risques pertinents soient couverts, il convient que la présente directive s'applique à tous les réseaux et systèmes informatiques. Les obligations imposées aux administrations publiques et aux acteurs du marché ne devraient cependant pas être applicables aux entreprises qui fournissent des réseaux de communication publics ou des services de communications électroniques accessibles au public au sens de la directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive «cadre»)[2], qui sont soumises aux dispositions particulières relatives à la sécurité et à l'intégrité énoncées à l'article 13 *bis* de ladite directive, ni aux fournisseurs de services de confiance.

(6) Les moyens existants ne sont pas suffisants pour assurer un niveau élevé de SRI 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'UE. Les niveaux de protection des particuliers et des entreprises sont donc inégaux, ce qui porte atteinte au niveau global de SRI dans l'Union. En outre, l'absence d'exigences minimales communes applicables aux administrations publiques et aux acteurs du marché rend impossible la création d'un mécanisme général de coopération efficace au niveau de l'Union.

(7) Il faut donc, pour faire face efficacement aux problèmes actuels dans le domaine de la sécurité des réseaux et de l'information, adopter une approche globale au niveau de l'Union qui couvrira des exigences minimales communes en matière de renforcement des capacités et de planification, l'échange d'informations et la coordination des actions, ainsi que des exigences minimales communes en matière de sécurité pour tous les acteurs du marché concernés et les administrations publiques.

(8) Les dispositions de la présente directive ne devraient pas porter atteinte à la possibilité donnée à chaque État membre d'adopter les mesures nécessaires pour garantir la protection de ses intérêts essentiels en matière de sécurité, assurer l'ordre public et la sécurité publique et permettre la recherche, la détection et la poursuite d'infractions pénales. Conformément à l’article 346 du TFUE, aucun État membre n’est tenu de fournir des renseignements dont il estimerait la divulgation contraire aux intérêts essentiels de sa sécurité.

(9) Pour atteindre un niveau commun élevé de sécurité des réseaux et de l'information et le maintenir, chaque État membre devrait se doter d'une stratégie nationale en matière de SRI définissant les objectifs stratégiques et les actions politiques concrètes à mettre en œuvre. Il convient de mettre en place, au niveau national, des plans de coopération en matière de SRI qui soient conformes aux exigences essentielles afin de disposer de moyens d'intervention d'un niveau permettant une coopération réelle et efficace, au niveau national comme à celui de l'Union, en cas d'incident.

[2] JO L 108 du 24.4.2002, p. 33.

(10) Pour que les dispositions adoptées en vertu de la présente directive puissent être effectivement mises en œuvre, il convient d'établir ou de désigner, dans chaque État membre, un organisme responsable de la coordination des aspects relatifs à la SRI et servant d'interlocuteur pour la coopération transfrontière au niveau de l'Union. Ces organismes devraient être dotés de ressources techniques, financières et humaines, suffisantes pour pouvoir s'acquitter de manière efficace et efficiente des tâches qui leur sont dévolues et atteindre ainsi les objectifs de la présente directive.

(11) Tous les États membres devraient disposer de moyens suffisants, sur les plans technique et organisationnel, pour prévenir et détecter les incidents et risques liés aux réseaux et systèmes informatiques et prendre les mesures d'intervention et d'atténuation nécessaires. Il convient, par conséquent, de mettre en place dans tous les États membres des équipes d'intervention en cas d'urgence informatique (CERT) opérationnelles et conformes aux exigences essentielles afin de garantir l'existence de moyens effectifs et compatibles pour gérer les incidents et les risques et d'assurer une coopération efficace au niveau de l'Union.

(12) En se fondant sur les progrès significatifs accomplis au sein du Forum européen des États membres pour favoriser les discussions et les échanges de bonnes pratiques en matière de sécurité, et notamment l'élaboration de principes relatifs à la coopération européenne en cas de crise dans le domaine de la cybersécurité, les États membres et la Commission devraient constituer un réseau leur permettant de rester en liaison permanente et fournissant un cadre à leur coopération. Ce mécanisme de coopération sécurisé et efficace devrait garantir, au niveau de l'UE, des actions structurées et coordonnées en matière d'échange d'informations, de détection et d'intervention.

(13) L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) devrait assister les États membres et la Commission en mettant à leur disposition son expérience et ses conseils et en facilitant l'échange des meilleures pratiques. En particulier, la Commission devrait consulter l'ENISA en ce qui concerne l'application de la présente directive. Pour faire en sorte que les États membres et la Commission soient informés efficacement et en temps voulu, un mécanisme d'alerte rapide sur les incidents et les risques devrait être mis en place dans le cadre du réseau de coopération. Afin de développer les moyens disponibles et la connaissance dans les États membres, le réseau de coopération devrait aussi être un outil d'échange des meilleures pratiques, qui aide ses membres à renforcer leurs capacités et dirige l'organisation d'examens par les pairs et d'exercices de SRI.

(14) Une infrastructure sécurisée de partage des informations devrait être mise en place de manière à permettre l'échange d'informations sensibles et confidentielles au sein du réseau de coopération. Sans préjudice de leur obligation de notifier au réseau de coopération les incidents et les risques ayant une importance pour l'Union, seuls les États membres prouvant qu'ils disposent des ressources et processus techniques, financiers et humains et des infrastructures leur permettant de participer de manière efficace, efficiente et sûre au réseau devraient avoir accès aux informations confidentielles d'autres États membres.

(15) Étant donné que la plupart des réseaux et systèmes informatiques sont exploités par des intérêts privés, il est essentiel d'établir une coopération entre secteur public et secteur privé. Il convient d'encourager les acteurs du marché à mettre en place leurs propres mécanismes informels de coopération pour garantir la SRI. Ils devraient

également coopérer avec le secteur public et échanger des informations et des meilleures pratiques en contrepartie d'une assistance opérationnelle en cas d'incident.

(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.

(17) Lorsque des informations sont considérées comme confidentielles conformément à la réglementation nationale ou de l'Union en matière de secret des affaires, cette confidentialité est garantie lors de l'exécution des activités et de la réalisation des objectifs énoncés par la présente directive.

(18) La Commission et les États membres devraient, en se fondant notamment sur l'expérience acquise au niveau national en matière de gestion des crises, et en coopération avec l'ENISA, mettre en place un plan européen de coopération en matière de SRI définissant des mécanismes de coopération en vue de faire face aux menaces et incidents dans ce domaine. Il convient de tenir dûment compte de ce plan pour le fonctionnement du mécanisme d'alerte rapide au sein du réseau de coopération.

(19) L'activation du mécanisme d'alerte rapide dans le réseau ne devrait être obligatoire que si l'ampleur et la gravité de l'incident ou du risque en question est significative ou susceptible de le devenir au point de nécessiter une information ou une coordination de l'intervention au niveau de l'Union. Par conséquent, les alertes rapides devraient concerner uniquement les incidents ou risques réels ou potentiels qui évoluent rapidement, excèdent la capacité nationale d'intervention ou touchent plusieurs États membres. Toutes les informations pertinentes pour l'appréciation du risque ou de l'incident devraient être communiquées au réseau de coopération afin de permettre une évaluation correcte.

(20) Lorsqu'un message d'alerte rapide et une évaluation leur sont transmis, les autorités compétentes devraient décider d'une intervention coordonnée dans le cadre du plan de coopération en matière de SRI de l'Union. Il convient d'informer les autorités compétentes ainsi que la Commission des mesures adoptées au niveau national au titre de l'intervention coordonnée.

(21) Étant donné que les problèmes de SRI ont une dimension mondiale, il est nécessaire de renforcer la coopération internationale pour améliorer les normes de sécurité et les échanges d'informations et pour promouvoir une approche commune au niveau mondial en ce qui concerne les problèmes de SRI.

(22) C'est, dans une large mesure, aux administrations publiques et aux acteurs du marché qu'incombe la responsabilité de garantir la SRI. Il convient de promouvoir et de faire évoluer, au moyen d'exigences réglementaires appropriées et de pratiques sectorielles volontaires, une culture de la gestion des risques impliquant une analyse des risques et l'application de mesures de sécurité adaptées aux risques encourus. Il est aussi essentiel que les règles soient les mêmes partout pour que le réseau de coopération fonctionne réellement et que la coopération entre tous les États membres soit effective.

(23) En vertu de la directive 2002/21/CE, les entreprises qui fournissent des réseaux de communication publics ou des services de communications électroniques accessibles au public sont tenues de prendre les mesures appropriées pour garantir leur sécurité et leur intégrité. Cette directive introduit aussi des obligations de notification en cas

d'atteinte à la sécurité et de perte d'intégrité. En vertu de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive «vie privée et communications électroniques»)[3], le fournisseur d'un service de communications électroniques accessible au public doit prendre les mesures d'ordre technique et organisationnel appropriées afin de garantir la sécurité de ses services.

(24) Ces obligations devraient être étendues, au-delà du secteur des communications électroniques, aux principaux prestataires de services de la société de l'information au sens de la directive 98/34/CE du Parlement européen et du Conseil du 22 juin 1998 prévoyant une procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information[4], sur lesquels reposent des services de la société de l'information en amont ou des activités en ligne, tels que les plateformes de commerce électronique, les passerelles de paiement par internet, les réseaux sociaux, les moteurs de recherche, les services informatiques en nuage ou les magasins d'applications en ligne. Toute perturbation de ces services génériques de la société de l'information empêche la fourniture d'autres services de la société de l'information dont ils représentent des composantes sous-jacentes essentielles. Les développeurs de logiciels et les fabricants de matériel ne sont pas des prestataires de services de la société de l'information et sont par conséquent exclus. Ces obligations devraient aussi être étendues aux administrations publiques et aux opérateurs d'infrastructures critiques qui sont très dépendants des technologies de l'information et des communications et qui sont essentiels au maintien de fonctions économiques ou sociétales vitales telles que l'approvisionnement en électricité et en gaz naturel, les transports, les établissements de crédit, les bourses de valeurs et les soins de santé. Toute perturbation de ces réseaux et systèmes informatiques aurait une incidence négative sur le marché intérieur.

(25) Les mesures techniques et organisationnelles imposées aux administrations publiques et aux acteurs du marché ne devraient pas impliquer la conception, le développement ou la fabrication selon des modalités précises d'un produit TIC commercial particulier.

(26) Les administrations publiques et les acteurs du marché devraient garantir la sécurité des réseaux et systèmes placés sous leur contrôle. Il s'agit principalement de systèmes et réseaux privés qui sont gérés par leurs propres services informatiques ou dont la gestion de la sécurité a été sous-traitée. Les obligations en matière de sécurité et de notification devraient s'appliquer aux administrations publiques et acteurs du marché concernés, que la maintenance de leurs réseaux et systèmes informatiques soient assurée en interne par leurs propres services ou qu'elle soit sous-traitée.

(27) Pour éviter que la charge financière et administrative imposée aux utilisateurs et opérateurs de petite taille ne soit excessive, les exigences devraient être proportionnées aux risques que présente le réseau ou le système informatique concerné, compte tenu de l'état le plus avancé de la technique en ce qui concerne ces mesures. Ces exigences ne devraient pas être applicables aux micro-entreprises.

(28) Les autorités compétentes devraient veiller à préserver des canaux informels et dignes de confiance pour le partage d'informations entre les acteurs du marché et entre les

[3] JO L 201 du 31.7.2002, p. 37.
[4] JO L 204 du 21.7.1998, p. 37.

secteurs public et privé. La divulgation d'informations sur les incidents signalés aux autorités compétentes devrait être le reflet d'un compromis entre l'intérêt, pour le public, d'être informé des menaces et les éventuelles conséquences néfastes, pour les administrations publiques et les acteurs du marché signalant les incidents, en termes d'image comme sur le plan commercial. Lorsqu'elles mettent en œuvre les obligations de notification, les autorités compétentes devraient être particulièrement attentives à la nécessité de préserver la stricte confidentialité des informations sur les vulnérabilités des produits avant la publication des mises à jour de sécurité appropriées.

(29) Ces autorités devraient disposer des moyens nécessaires à l'exécution de leurs tâches, et notamment des pouvoirs leur permettant d'obtenir des administrations publiques et des acteurs du marché des informations suffisantes pour évaluer le niveau de sécurité des réseaux et systèmes informatiques, ainsi que des données fiables et complètes relatives aux incidents qui ont eu une incidence sur le fonctionnement des réseaux et systèmes informatiques.

(30) Dans bien des cas, la cause sous-jacente d'un incident est une activité criminelle. Certains incidents sont susceptibles de constituer des infractions pénales même si les éléments qui en attestent ne sont pas suffisamment probants dès le départ. Dans ce contexte, toute réponse efficace et complète à la menace que représentent les incidents de sécurité devrait s'appuyer sur une coopération appropriée entre les autorités compétentes et les services répressifs. La promotion d'un environnement sûr, sécurisé et plus résilient exige que soient signalés aux services répressifs les incidents susceptibles de constituer des infractions pénales graves. Le caractère de grave infraction pénale de ces incidents devrait être évalué à la lumière de la législation de l'UE sur la cybercriminalité.

(31) Dans de nombreux cas, des données à caractère personnel sont compromises à la suite d'incidents. Dans de telles circonstances, les autorités compétentes et les autorités chargées de la protection des données devraient coopérer et échanger des informations sur tous les aspects pertinents de la lutte contre les atteintes aux données à caractère personnel à la suite d'incidents. Les États membres doivent mettre en œuvre l'obligation de notifier les incidents de sécurité d'une manière qui réduise au minimum la charge administrative lorsque l'incident de sécurité porte aussi atteinte à des données à caractère personnel conformément au règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[5]. L'ENISA pourrait, en liaison avec les autorités compétentes et les autorités chargées de la protection des données, apporter son concours en élaborant des formulaires et des mécanismes pour l'échange d'informations, ce qui éviterait la duplication des formulaires de notification. Un formulaire de notification unique faciliterait le signalement des incidents qui portent atteinte à des données à caractère personnel, ce qui réduirait la charge administrative pesant sur les entreprises et les administrations publiques.

(32) La normalisation des exigences en matière de sécurité est un processus guidé par le marché. Pour assurer l'application convergente des normes en matière de sécurité, les États membres devraient encourager le respect de normes précises ou la conformité à ces dernières afin de garantir un niveau élevé de sécurité au niveau de l'Union. À cette

[5] SEC (2012) 72 final

fin, il pourrait être nécessaire d'élaborer des projets de normes harmonisées, en se conformant aux dispositions du règlement (UE) n° 1025/2012 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne, modifiant les directives 89/686/CEE et 93/15/CEE du Conseil ainsi que les directives 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE et 2009/105/CE du Parlement européen et du Conseil et abrogeant la décision 87/95/CEE du Conseil et la décision n° 1673/2006/CE du Parlement européen et du Conseil[6].

(33) Les dispositions de la présente directive devraient être réexaminées périodiquement par la Commission, notamment en vue de déterminer s'il est nécessaire de les modifier pour tenir compte de l'évolution des technologies ou de la situation des marchés.

(34) En vue de permettre le bon fonctionnement du réseau de coopération, le pouvoir d'adopter des actes visé à l'article 290 du TFUE devrait être délégué à la Commission en ce qui concerne la définition des critères qu'un État membre doit respecter pour être autorisé à participer au système sécurisé d'échange d'informations, la définition plus précise des événements déclenchant l'activation du mécanisme d'alerte rapide, et la définition des circonstances dans lesquelles les acteurs du marché et les administrations publiques sont tenus de notifier les incidents.

(35) Il importe particulièrement que la Commission procède aux consultations appropriées au cours de ses travaux préparatoires, y compris au niveau des experts. Il convient que, lorsqu'elle prépare et élabore des actes délégués, la Commission veille à ce que les documents pertinents soient transmis simultanément, en temps utile et de façon appropriée, au Parlement européen et au Conseil.

(36) Afin de garantir des conditions uniformes d'application de la présente directive, il y a lieu de conférer des compétences d'exécution à la Commission en ce qui concerne la coopération entre les autorités nationales compétentes et la Commission au sein du réseau de coopération, l'accès à l'infrastructure sécurisée de partage des informations, le plan de coopération de l'Union en matière de SRI, les formats et procédures applicables à l'information du public en cas d'incident et les normes et/ou spécifications techniques relatives à la SRI. Il convient que ces compétences soient exercées conformément au règlement (UE) n° 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution[7] par la Commission.

(37) Pour l'application de la présente directive, la Commission devrait communiquer comme il se doit avec les comités sectoriels et organismes pertinents établis au niveau de l'UE, notamment dans les domaines de l'énergie, des transports et de la santé.

(38) Les informations considérées comme confidentielles par une autorité compétente, conformément à la réglementation de l'Union et à la réglementation nationale en matière de secret des affaires, ne devraient être échangées avec la Commission et d'autres autorités compétentes que si cet échange est strictement nécessaire à l'application des dispositions de la présente directive. Les informations échangées devraient se limiter au minimum nécessaire et être proportionnées à l'objectif de cet échange.

---

6 JO L 316 du 14.11.2012, p. 12.

7 JO L 55 du 28.2.2011, p. 13.

(39) Le partage des informations sur les risques et incidents au sein du réseau de coopération et le respect des exigences relatives à la notification des incidents aux autorités nationales compétentes peuvent nécessiter le traitement de données à caractère personnel. Ce traitement est nécessaire à l'exécution de la mission d'intérêt public qui est celle de la présente directive et il est donc légitime en vertu de l'article 7 de la directive 95/46/CE. Il ne constitue pas, au regard de ces objectifs légitimes, une intervention disproportionnée et intolérable qui porterait atteinte à la substance même du droit à la protection des données à caractère personnel consacré à l'article 8 de la charte des droits fondamentaux. Les dispositions du règlement (CE) n° 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission s'appliquent, le cas échéant, pour ce qui est de l'application de la présente directive[8]. Lorsqu'un traitement des données à caractère personnel est effectué par les institutions et organes de l'Union aux fins de la mise en œuvre de la présente directive, il est conforme aux dispositions du règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données.

(40) Étant donné que les objectifs de la présente directive, à savoir garantir un niveau élevé de SRI dans l'Union, ne peuvent pas être réalisés de manière suffisante par les seuls États membres et peuvent donc, en raison des effets de l'action, être mieux atteints au niveau de l'Union, celle-ci peut prendre des mesures, conformément au principe de subsidiarité consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité tel qu'énoncé audit article, la présente directive n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

(41) La présente directive respecte les droits fondamentaux et les principes reconnus par la Charte des droits fondamentaux de l'Union européenne et notamment le droit au respect de la vie privée et des communications, le droit à la protection des données à caractère personnel, le droit à la liberté d'entreprise, le droit de propriété ainsi que le droit à un recours effectif et à un procès équitable. La présente directive doit être mise en œuvre conformément à ces droits et principes.

ONT ADOPTÉ LA PRÉSENTE DIRECTIVE:

## CHAPITRE I

## DISPOSITIONS GÉNÉRALES

*Article premier*

Objet et champ d'application

1. La présente directive établit des mesures visant à assurer un niveau commun élevé de sécurité des réseaux et de l'information (SRI) dans l'Union.

2. À cette fin:

[8] JO L 145 du 31.5.2001, p. 43.

(a) elle fixe des obligations à tous les États membres en ce qui concerne la prévention et la gestion de risques et incidents touchant les réseaux et systèmes informatiques ainsi que les interventions en cas d'événement de ce type;

(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;

(c) elle établit des exigences en matière de sécurité pour les acteurs du marché et les administrations publiques.

3. Les exigences en matière de sécurité prévues à l'article 14 ne s'appliquent ni aux entreprises qui fournissent des réseaux de communication publics ou des services de communications électroniques accessibles au public au sens de la directive 2002/21/CE, qui sont soumises aux dispositions particulières relatives à la sécurité et à l'intégrité énoncées aux articles 13 *bis* et 13 *ter* de ladite directive, ni aux fournisseurs de services de confiance.

4. La présente directive ne porte pas atteinte aux dispositions de la législation de l'UE sur la cybercriminalité ni à celles de la directive 2008/114/CE du Conseil du 8 décembre 2008 concernant le recensement et la désignation des infrastructures critiques européennes ainsi que l'évaluation de la nécessité d'améliorer leur protection[9].

5. Elle ne porte pas non plus atteinte aux dispositions de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[10], de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et du règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[11].

6. Le partage des informations au sein du réseau de coopération visé au chapitre III et les notifications d'incidents de SRI en vertu de l'article 14 peuvent nécessiter le traitement de données à caractère personnel. Ce traitement, qui est nécessaire à l'exécution de la mission d'intérêt public qui est celle de la présente directive, est autorisé par l'État membre conformément à l'article 7 de la directive 95/46/CE et à la directive 2002/58/CE, tels que transposés en droit national.

*Article 2*

Harmonisation minimale

9 JO L 345 du 23.12.2008, p. 75.
10 JO L 281 du 23.11.1995, p. 31.
11 SEC (2012) 72 final.

Les États membres ont la faculté d'adopter ou de maintenir des dispositions garantissant un niveau de sécurité plus élevé, sans préjudice de leurs obligations découlant de la législation de l'Union.

*Article 3*

Définitions

Aux fins de la présente directive, on entend par:

(1) «réseau et système informatique»,

(a) un réseau de communications électroniques au sens de la directive 2002/21/CE et

(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

(c) les données informatiques stockées, traitées, récupérées ou transmises par les éléments visés aux points (a) et (b) derniers en vue de leur fonctionnement, utilisation, protection et maintenance.

(2) «sécurité», la capacité d'un réseau et d'un système informatique de résister, à un niveau de confiance donné, à des événements accidentels ou à des actions malveillantes qui compromettent la disponibilité, l'authenticité, l'intégrité et la confidentialité de données stockées ou transmises, et des services connexes que ces réseaux et systèmes offrent ou qu'ils rendent accessibles;

(3) «risque», toute circonstance ou tout événement ayant une incidence négative potentielle sur la sécurité;

(4) «incident», toute circonstance ou tout événement ayant une incidence négative réelle sur la sécurité;

(5) «service de la société de l'information», un service au sens de l'article 1er, point 2, de la directive 98/34/CE;

(6) «plan de coopération en matière de SRI», un plan établissant un cadre pour les rôles, responsabilités et procédures opérationnelles visant à maintenir ou à rétablir le fonctionnement des réseaux et systèmes informatiques en cas de risque ou d'incident;

(7) «gestion d'incident», toutes les procédures utiles à l'analyse, au confinement et à l'intervention en cas d'incident;

(8) «acteur du marché»,

(a) un prestataire de services de la société de l'information qui permet la fourniture d'autres services de la société de l'information dont une liste non exhaustive 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 et de la santé, énumérées dans une liste non exhaustive qui figure à l'annexe II.

(9) «norme», une norme visée dans le règlement (UE) n° 1025/2012;

(10) «spécification», une spécification visée dans le règlement (UE) n° 1025/2012;

(11) «prestataire de service de confiance», une personne physique ou morale qui fournit tout service électronique consistant en la création, la vérification, la validation, le traitement et la conservation de signatures électroniques, de cachets électroniques, d'horodatages électroniques, de documents électroniques, de services de fourniture électronique, d'authentification de site web et de certificats électroniques, y compris de certificats de signature électronique et de cachet électronique.

## CHAPITRE II

## CADRES NATIONAUX DE SÉCURITÉ DES RÉSEAUX ET DE L'INFORMATION

*Article 4*

Principe

Les États membres assurent, conformément à la présente directive, un niveau élevé de sécurité des réseaux et des systèmes informatiques sur leur territoire.

*Article 5*

Stratégies nationales et plans nationaux de coopération en matière de SRI

1. Chaque État membre adopte une stratégie nationale en matière de SRI qui définit les objectifs stratégiques et les mesures politiques et réglementaires concrètes visant à parvenir à un niveau élevé de sécurité des réseaux et de l'information et à le maintenir. Les principaux aspects sur lesquels porte la stratégie nationale en matière de SRI sont les suivants:

(a) la définition des objectifs et des priorités de la stratégie fondée sur une analyse actualisée des risques et des incidents;

(b) un cadre de gouvernance permettant d'atteindre les objectifs stratégiques et les priorités, fournissant notamment une définition claire des rôles et des responsabilités des organismes gouvernementaux et des autres acteurs pertinents;

(c) l'inventaire des mesures générales en matière de préparation, d'intervention et de récupération, et notamment des mécanismes de coopération entre les secteurs public et privé;

(d) la mention des programmes d'éducation, de sensibilisation et de formation;

(e) les plans de recherche et développement et la description de la manière dont ils tiennent compte des priorités recensées.

2. La stratégie nationale en matière de SRI comporte un plan national de coopération en matière de SRI qui satisfait au moins aux exigences suivantes:

(a) un plan d'évaluation des risques permettant de recenser les risques et d'évaluer l'impact des incidents potentiels;

(b) la définition des rôles et des responsabilités des différents acteurs concernés par la mise en œuvre du plan;

(c) la définition des processus de coopération et de communication qui garantissent la prévention, la détection, l'intervention, la réparation et la récupération, avec une modulation en fonction du niveau d'alerte;

(d) une feuille de route concernant des exercices et formations en matière de SRI pour renforcer et valider le plan et le mettre à l'épreuve. Les enseignements tirés seront ensuite intégrés dans les mises à jour du plan.

3. La stratégie nationale et le plan national de coopération en matière de SRI seront communiqués à la Commission dans le mois suivant leur adoption.

*Article 6*

Autorités nationales compétentes en matière de sécurité des réseaux et systèmes informatiques

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

2. Les autorités compétentes contrôlent l'application de la présente directive au niveau national et contribuent à son application cohérente dans l'ensemble de l'Union.

3. Les États membres veillent à ce que les autorités compétentes disposent de ressources techniques, financières et humaines suffisantes pour pouvoir s'acquitter de leurs tâches de manière efficace et efficiente et atteindre ainsi les objectifs de la présente directive. Les États membres font en sorte que les autorités compétentes puissent coopérer de manière efficace, efficiente et sûre par l'intermédiaire du réseau visé à l'article 8.

4. Les États membres veillent à ce que les autorités compétentes reçoivent les notifications d'incidents des administrations publiques et des acteurs du marché conformément à l'article 14, paragraphe 2, et à ce qu'elles disposent des compétences de mise en œuvre et d’exécution visées à l'article 15.

5. Les autorités compétentes consultent les services répressifs nationaux compétents et les autorités chargées de la protection des données et, le cas échéant, coopèrent avec eux.

6. Chaque État membre informe sans retard la Commission de la désignation de l'autorité compétente et des tâches confiées à cette dernière et de toute modification

ultérieure les concernant. Chaque État membre rend publique la désignation de l'autorité compétente.

*Article 7*

Équipes d'intervention en cas d'urgence informatique (CERT)

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.

2. Les États membres veillent à ce que les CERT disposent de ressources techniques, financières et humaines suffisantes pour pouvoir s'acquitter efficacement des tâches énumérées au point (2) de l'annexe I.

3. Les États membres font en sorte que les CERT puissent compter sur une infrastructure d'information et de communication sécurisée et résiliente au niveau national, dont la compatibilité et l'interopérabilité avec le système sécurisé d'échange d'informations visé à l'article 9 soient garanties.

4. Les États membres informent la Commission des ressources et du mandat des CERT, ainsi que de leurs processus de gestion des incidents.

5. Les CERT sont placées sous la surveillance de l'autorité compétente, qui procède régulièrement à un examen visant à établir que leurs ressources et leur mandat sont adaptés et que leur processus de gestion des incidents est efficace.

## CHAPITRE III

## COOPÉRATION ENTRE LES AUTORITÉS COMPÉTENTES

*Article 8*

Réseau de coopération

1. Les autorités compétentes et la Commission constituent un réseau («réseau de coopération») pour coopérer dans la lutte contre les risques et incidents touchant les réseaux et systèmes informatiques.

2. Ce réseau permet à la Commission et aux autorités compétentes de rester en liaison permanente. Lorsque c'est nécessaire, l'Agence européenne chargée de la sécurité des réseaux et de l'information («ENISA») assiste le réseau de coopération en mettant à sa disposition son expérience et ses conseils.

3. Au sein du réseau de coopération, les autorités compétentes:

   (a) diffusent les messages d'alerte rapide sur les risques et incidents conformément à l'article 10;

   (b) assurent une intervention coordonnée conformément à l'article 11;

(c) publient régulièrement, sur un site web commun, des informations non confidentielles sur les alertes rapides et les interventions coordonnées en cours;

(d) procèdent, à la demande d'un État membre ou de la Commission, à un examen et une évaluation communs d'un ou de plusieurs plans de coopération et stratégies nationaux en matière de SRI visés à l'article 5, dans le champ d'application de la présente directive;

(e) procèdent, à la demande d'un État membre ou de la Commission, à un examen et une évaluation communs de l'efficacité des CERT, notamment lorsque des exercices de SRI sont exécutés au niveau de l'Union;

(f) coopèrent et échangent des informations sur tous les aspects pertinents avec le Centre européen de lutte contre la cybercriminalité au sein d'Europol, et avec d'autres organismes européens concernés, notamment dans le domaine de la protection des données, de l'énergie, des transports, des services bancaires, des bourses de valeurs et de la santé;

(g) échangent des informations et de bonnes pratiques, entre elles et avec la Commission, et s'assistent mutuellement en ce qui concerne le renforcement des capacités de SRI;

(h) organisent régulièrement des examens par les pairs portant sur les moyens et l'état de préparation;

(i) organisent des exercices de SRI au niveau de l'Union et participent, le cas échéant, à des exercices de SRI internationaux.

4. La Commission établit, au moyen d'actes d'exécution, les modalités nécessaires pour faciliter la coopération entre les autorités compétentes et la Commission visée aux paragraphes 2 et 3. Ces actes d'exécution sont adoptés en conformité avec la procédure de consultation visée à l'article 19, paragraphe 2.

*Article 9*

Système sécurisé d'échange d'informations

1. L'échange d'informations sensibles et confidentielles au sein du réseau de coopération se déroule dans le cadre d'une infrastructure sécurisée de partage des informations.

2. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 18 en ce qui concerne la définition des critères qu'un État membre doit respecter pour être autorisé à participer au système sécurisé d'échange d'informations, pour ce qui a trait:

(a) à la disponibilité d'une infrastructure d'information et de communication sécurisée et résiliente au niveau national, dont la compatibilité et l'interopérabilité avec le réseau de coopération soient garanties conformément à l'article 7, paragraphe 3, et

(b) à l'existence de ressources et processus techniques, financiers et humains suffisants pour permettre aux autorités compétentes et aux CERT de participer de manière efficace, efficiente et sûre au système sécurisé d'échange d'informations au titre de l'article 6, paragraphe 3, de l'article 7, paragraphes 2 et 3.

3. La Commission adopte, au moyen d'actes d'exécution, des décisions relatives à l'accès des États membres à cette infrastructure sécurisée, conformément aux critères visés aux paragraphes 2 et 3. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 19, paragraphe 3.

*Article 10*
Alerte rapide

1. Les autorités compétentes ou la Commission établissent, au sein du réseau de coopération, un mécanisme d'alerte rapide pour les risques et incidents qui remplissent au moins une des conditions suivantes:

(a) leur ampleur s'accroît ou peut s'accroître rapidement;

(b) ils excèdent ou peuvent excéder la capacité nationale d'intervention;

(c) ils touchent ou peuvent toucher plusieurs États membres.

2. Dans le cadre du mécanisme d'alerte rapide, les autorités compétentes et la Commission communiquent toutes les informations pertinentes en leur possession qui peuvent être utiles pour évaluer le risque ou l'incident.

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.

4. Lorsque le risque ou l'incident qui a déclenché l'activation du mécanisme d'alerte rapide est susceptible de constituer une infraction pénale, les autorités nationales compétentes ou la Commission en informent le Centre européen de lutte contre la cybercriminalité d'Europol.

5. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 18 aux fins de préciser davantage les risques et incidents déclenchant l'activation du mécanisme d'alerte rapide conformément au paragraphe 1.

*Article 11*
Intervention coordonnée

1. Après l'activation du mécanisme d'alerte rapide visé à l'article 10, les autorités compétentes décident, après évaluation des informations pertinentes, d'une intervention coordonnée conformément au plan de coopération de l'Union en matière de SRI visé à l'article 12.

2. Les différentes mesures adoptées au niveau national au titre de l'intervention coordonnée sont communiquées au réseau de coopération.

*Article 12*

Plan de coopération de l'Union en matière de SRI

1. La Commission est habilitée à adopter, au moyen d'actes d'exécution, un plan de coopération de l'Union en matière de SRI. Ces actes d'exécution sont adoptés selon la procédure d'examen visée à l'article 19, paragraphe 3.

2. Le plan de coopération de l'Union en matière de SRI prévoit:

   (a) aux fins de l'application de l'article 10:

   – une définition du format et des procédures applicables à la collecte et au partage, par les autorités compétentes, d'informations compatibles et comparables sur les risques et incidents,

   – une définition des procédures et critères d'évaluation des risques et incidents par le réseau de coopération.

   (b) les processus applicables à l'intervention coordonnée au titre de l'article 11, et notamment la détermination des rôles, des responsabilités et des procédures de coopération;

   (c) une feuille de route concernant les exercices et formations en matière de SRI pour renforcer et valider le plan et le mettre à l'épreuve;

   (d) un programme de transfert des connaissances entre les États membres en ce qui concerne le renforcement des capacités et l'apprentissage entre pairs,

   (e) un programme de sensibilisation et de formation entre les États membres.

3. Le plan de coopération de l'Union en matière de SRI est adopté au plus tard un an après l'entrée en vigueur de la présente directive et est révisé régulièrement.

*Article 13*

Coopération internationale

L'Union peut conclure, avec des pays tiers ou des organisations internationales, des accords internationaux qui permettent et organisent leur participation à certaines activités du réseau de coopération, sans préjudice des activités informelles de coopération internationale offertes au réseau de coopération. Ces accords tiennent compte de la nécessité d'assurer un niveau suffisant de protection des données à caractère personnel diffusées au sein du réseau de coopération.

**CHAPITRE IV**

## SÉCURITÉ DES RÉSEAUX ET SYSTÈMES INFORMATIQUES DES ADMINISTRATIONS PUBLIQUES ET DES ACTEURS DU MARCHÉ

*Article 14*

Exigences de sécurité et notification d'incidents

1. Les États membres veillent à ce que les administrations publiques et les acteurs du marché prennent les mesures techniques et organisationnelles nécessaires pour gérer les risques qui menacent la sécurité des réseaux et systèmes informatiques qu'ils contrôlent et utilisent dans le cadre de leurs activités. Ces mesures garantissent un niveau de sécurité adapté au risque existant, compte tenu des possibilités techniques les plus avancées. Des mesures sont prises, en particulier, pour éviter les incidents touchant les réseaux et systèmes informatiques et réduire au minimum leur impact sur les services essentiels qu'ils fournissent, de manière à garantir la continuité des services qui dépendent de ces réseaux et systèmes.

2. Les États membres veillent à ce que les administrations publiques et les acteurs du marché notifient à l'autorité compétente les incidents qui ont un impact significatif sur la sécurité des services essentiels qu'ils fournissent.

3. Les exigences visées aux paragraphes 1 et 2 s'appliquent à tous les acteurs du marché fournissant des services dans l'Union européenne.

4. L'autorité compétente peut informer le public, ou demander aux administrations publiques et aux acteurs du marché de le faire, lorsqu'elle juge qu'il est dans l'intérêt général de divulguer les informations relatives à l'incident. Une fois par an, l'autorité compétente soumet au réseau de coopération un rapport succinct sur les notifications reçues et l'action engagée conformément au présent paragraphe.

5. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 18 en ce qui concerne la définition des circonstances dans lesquelles les administrations publiques et les acteurs du marché sont tenus de notifier les incidents.

6. Sous réserve de tout acte délégué adopté en vertu du paragraphe 5, les autorités compétentes peuvent adopter des lignes directrices et, le cas échéant, formuler des instructions relatives aux circonstances dans lesquelles les administrations publiques et les acteurs du marché sont tenus de notifier les incidents.

7. La Commission est habilitée à définir, au moyen d'actes d'exécution, les formats et procédures applicables aux fins de l'application du paragraphe 2. Ces actes d'exécution sont adoptés selon la procédure d'examen visée à l'article 19, paragraphe 3

8. Les paragraphes 1 et 2 ne s'appliquent pas aux micro-entreprises telles qu'elles sont définies dans la recommandation de la Commission 2003/361/CE du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises[12].

[12] JO L 124 du 20.5.2003, p. 36.

*Article 15*

Mise en œuvre et exécution

1. Les États membres veillent à ce que les autorités compétentes aient tous les pouvoirs nécessaires leur permettant d'enquêter sur les cas dans lesquels les administrations publiques ou les acteurs du marché ne respectent pas les obligations qui leur incombent en vertu de l'article 14 et sur les effets de ce non-respect sur la sécurité des réseaux et systèmes informatiques.

2. Les États membres veillent à ce que les autorités compétentes aient le pouvoir d'exiger des administrations publiques ou des acteurs du marché qu'ils:

   (a) fournissent les informations nécessaires pour évaluer la sécurité de leurs réseaux et systèmes informatiques, y compris les documents relatifs à leurs politiques de sécurité;

   (b) 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.

3. Les États membres veillent à ce que les autorités compétentes aient le pouvoir de donner des instructions contraignantes aux administrations publiques et aux acteurs du marché.

4. Les autorités compétentes notifient aux services répressifs les incidents pouvant constituer une infraction pénale grave.

5. Les autorités compétentes coopèrent étroitement avec les autorités chargées de la protection des données en cas d'incident portant atteinte à des données à caractère personnel.

6. Les États membres veillent à ce que toute obligation imposée aux administrations publiques et aux acteurs du marché au titre du présent chapitre puisse faire l’objet d’un contrôle juridictionnel.

*Article 16*

Normalisation

1. Pour veiller à la convergence de la mise en œuvre des dispositions de l'article 14, paragraphe 1, les États membres encouragent l'utilisation des normes et/ou des spécifications pertinentes pour la sécurité des réseaux et de l'information.

2. La Commission établit, au moyen d'actes d'exécution, une liste des normes visées au paragraphe 1. Cette liste est publiée au *Journal officiel de l’Union européenne*.

## CHAPITRE V

## DISPOSITIONS FINALES

*Article 17*

Sanctions

1. Les États membres fixent des règles relatives aux sanctions applicables en cas d'infraction aux dispositions nationales adoptées en vertu de la présente directive et prennent toutes les mesures nécessaires pour que ces règles soient appliquées. Les sanctions ainsi prévues doivent être effectives, proportionnées et dissuasives. Les États membres notifient ces dispositions à la Commission au plus tard à la date de transposition de la présente directive en droit national, et toute modification ultérieure les concernant dans les meilleurs délais.

2. Lorsqu'un incident de sécurité concerne des données à caractère personnel, les États membres veillent à ce que les sanctions prévues soient conformes à celles que prévoit le règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[13].

*Article 18*

Exercice de la délégation

1. Le pouvoir d'adopter des actes délégués conféré à la Commission est soumis aux conditions fixées au présent article.

2. Le pouvoir d'adopter des actes délégués visés à l'article 9, paragraphe 2, à l'article 10, paragraphe 5, et à l'article 14, paragraphe 5, est conféré à la Commission. La Commission élabore un rapport relatif à la délégation de pouvoir, au plus tard neuf mois avant la fin de la période de cinq ans. La délégation de pouvoir est tacitement prolongée pour des périodes d'une durée identique, sauf si le Parlement européen ou le Conseil s'oppose à cette prolongation trois mois au plus tard avant la fin de chaque période.

3. La délégation de pouvoir visée à l'article 9, paragraphe 2, à l'article 10, paragraphe 5, et à l'article 14, paragraphe 5, peut être révoquée à tout moment par le Parlement européen ou par le Conseil. La décision de révocation met fin à la délégation de pouvoir qui y est précisée. La révocation prend effet le jour suivant celui de la publication de ladite décision au *Journal officiel de l'Union européenne* ou à une date ultérieure qui est précisée dans ladite décision. Elle n'affecte pas la validité des actes délégués déjà en vigueur.

4. Aussitôt qu'elle adopte un acte délégué, la Commission le notifie simultanément au Parlement européen et au Conseil.

5. Un acte délégué adopté en vertu de l'article 9, paragraphe 2, de l'article 10, paragraphe 5, et de l'article 14, paragraphe 5, n'entre en vigueur que si le Parlement européen ou le Conseil n'a pas exprimé d'objections dans un délai de deux mois à compter de la notification de cet acte au Parlement européen et au Conseil ou si, avant l'expiration de ce délai, le Parlement européen et le Conseil ont,

[13] SEC (2012) 72 final.

tous deux, informé la Commission de leur intention de ne pas exprimer d'objections. Ce délai est prolongé de deux mois à l'initiative du Parlement européen ou du Conseil.

*Article 19*

Comité

1. La Commission est assistée par un comité («comité de la sécurité des réseaux et de l'information»). Il s'agit d'un comité au sens du règlement (UE) n° 182/2011.

2. Lorsqu'il est fait référence au présent paragraphe, l'article 4 du règlement (UE) n° 182/2011 est applicable.

3. Lorsqu'il est fait référence au présent paragraphe, l'article 5 du règlement (UE) n° 182/2011 est applicable.

*Article 20*

Examen

La Commission réexamine périodiquement le fonctionnement de la présente directive et en rend compte au Parlement européen et au Conseil. Le premier rapport est présenté au plus tard trois ans après la date de transposition visée à l'article 21. À cet effet, la Commission peut demander des informations aux États membres, qui les communiquent sans délai indu.

*Article 21*

Transposition

1. Les États membres adoptent et publient, au plus tard [un an et demi après l'adoption], les dispositions législatives, réglementaires et administratives nécessaires pour se conformer à la présente directive. Ils communiquent immédiatement à la Commission le texte de ces dispositions.

   Ils appliquent ces mesures à partir de [un an et demi après l'adoption].

   Lorsque les États membres adoptent ces dispositions, celles-ci contiennent une référence à la présente directive ou sont accompagnées d'une telle référence lors de leur publication. Les modalités de cette référence sont arrêtées par les États membres.

2. Les États membres communiquent à la Commission le texte des dispositions essentielles de droit interne qu'ils adoptent dans le domaine couvert par la présente directive.

*Article 22*

Entrée en vigueur

La présente directive entre en vigueur le [vingtième] jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

*Article 23*

Destinataires

Les États membres sont destinataires de la présente directive.

Fait à Bruxelles, le

| | |
|---|---|
| *Par le Parlement européen* | *Par le Conseil* |
| *Le président* | *Le président* |

## ANNEXE I

**Obligations et tâches de l'équipe d'intervention en cas d'urgence informatique (CERT)**

Les obligations et tâches de la CERT doivent être correctement et clairement définies sur la base d'une politique ou réglementation nationale. Elles comprennent les éléments suivants:

(1) Obligations de la CERT

(a) La CERT doit veiller à la grande disponibilité de ses services de communication en évitant les points uniques de défaillance et en prévoyant plusieurs moyens pour être contactée et contacter autrui. De plus, les canaux de communication doivent être clairement précisés et bien connus des partenaires et collaborateurs.

(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.

(c) Les bureaux de la CERT et les systèmes informatiques utilisés doivent se trouver sur des sites sécurisés.

(d) Un système de gestion de la qualité est créé pour assurer le suivi des résultats obtenus par la CERT et favoriser un processus d'amélioration permanent. Il est fondé sur des outils de mesure clairement définis au nombre desquels figurent les niveaux de service et les indicateurs clés de performance.

(e) Continuité des opérations:

– La CERT est dotée d'un système approprié de gestion et de routage des demandes afin de faciliter les transferts.

– La CERT est dotée des effectifs adéquats afin de pouvoir garantir une disponibilité permanente.

– La CERT s'appuie sur une infrastructure dont la continuité est garantie. À cette fin, des systèmes redondants et un espace de travail de secours sont mis en place pour que la CERT puisse assurer un accès permanent aux moyens de communication.

(2) Tâches de la CERT

(a) Les tâches de la CERT comprennent au moins les éléments suivants:

– surveillance des incidents au niveau national,

– activation du mécanisme d'alerte rapide, diffusion de messages d'alerte, annonces et diffusion d'information sur les risques et incidents auprès des parties intéressées,

– intervention en cas d'incident,

– analyse dynamique des risques et incidents et conscience situationnelle,

– sensibilisation du public dans son ensemble aux risques liés aux activités en ligne,

– organisation de campagnes consacrées à la SRI.

(b) La CERT établit des relations de coopération avec le secteur privé.

(c) Pour faciliter la coopération, la CERT promeut l'adoption et l'utilisation de pratiques communes normalisées pour:

– les procédures de gestion des risques et incidents,

– les systèmes de classification des incidents, risques et informations,

– les taxinomies pour les outils de mesure,

– les formats d'échange des informations sur les risques, les incidents et les conventions de nommage des systèmes.

## ANNEXE II

### Liste des acteurs du marché

**visés à l'article 3, paragraphe 8, point a)**

1. Plateformes de commerce électronique

2. Passerelles de paiement par internet,

3. Réseaux sociaux

4. Moteurs de recherche

5. Services informatiques en nuage

6. Magasins d'applications en ligne

**visés à l'article 3, paragraphe 8, point b)**

1. Énergie (marchés de l'électricité et du gaz)

- fournisseurs d'électricité et de gaz
- gestionnaires de réseaux de distribution de gaz et/ou d'électricité et détaillants livrant aux clients finals
- gestionnaires de réseaux de transport de gaz naturel, exploitants d'installations de stockage et d'installations GPL
- gestionnaires de réseaux de transport d'électricité
- oléoducs et installations de stockage de pétrole
- opérateurs sur les marchés du gaz et de l'électricité
- exploitants d'installations de production, de raffinage et de traitement de pétrole et de gaz naturel

2. Transports

- transporteurs aériens (fret et passagers)
- transporteurs maritimes (sociétés de transports maritimes et côtiers de passagers et sociétés de transports maritimes et côtiers de marchandises)
- chemins de fer (gestionnaires d'infrastructures, entreprises intégrées et opérateurs de transports ferroviaires)
- aéroports
- ports

– opérateurs de contrôle de gestion du trafic

– services logistiques auxiliaires (a) entreposage et stockage, b) manutention du fret et c) autres services auxiliaires des transports.

3. Services bancaires: établissements de crédit conformément à l'article 4, paragraphe 1, de la directive 2006/48/CE.

4. Infrastructures de marchés financiers: bourses de valeurs et contrepartie centrale/chambres de compensation.

5. Secteur de la santé: établissements de soins de santé (y compris les hôpitaux et les cliniques privées) et autres entités fournissant des soins de santé.

# FICHE FINANCIÈRE LÉGISLATIVE

## 1. CADRE DE LA PROPOSITION/DE L'INITIATIVE

1.1. Dénomination de la proposition/de l'initiative

1.2. Domaines politiques concernés dans la structure GPA/EBA

1.3. Nature de la proposition/de l'initiative

1.4. Objectifs

1.5. Justification(s) de la proposition/de l'initiative

1.6. Durée et incidence financière

1.7. Mode(s) de gestion prévu(s)

## 2. MESURES DE GESTION

2.1. Dispositions en matière de suivi et de compte rendu

2.2. Système de gestion et de contrôle

2.3. Mesures de prévention des fraudes et irrégularités

## 3. INCIDENCE FINANCIÈRE ESTIMÉE DE LA PROPOSITION/DE L'INITIATIVE

3.1. Rubrique(s) du cadre financier pluriannuel et ligne(s) budgétaire(s) de dépenses concernée(s)

3.2. Incidence estimée sur les dépenses

*3.2.1. Synthèse de l'incidence estimée sur les dépenses*

*3.2.2. Incidence estimée sur les crédits opérationnels*

*3.2.3. Incidence estimée sur les crédits de nature administrative*

*3.2.4. Compatibilité avec le cadre financier pluriannuel actuel*

*3.2.5. Participation de tiers au financement*

3.3. Incidence estimée sur les recettes

# FICHE FINANCIÈRE LÉGISLATIVE

## 1. CADRE DE LA PROPOSITION/DE L'INITIATIVE

### 1.1. Dénomination de la proposition/de l'initiative

Proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé de sécurité des réseaux et de l'information dans l'Union

### 1.2. Domaine politique concerné dans la structure GPA/EBA[37]

Réseaux de communication, contenu et technologies

### 1.3. Nature de la proposition/de l'initiative

☒ La proposition/l'initiative porte sur une **action nouvelle**

☐ La proposition/l'initiative porte sur une **action nouvelle suite à un projet pilote/une action préparatoire**[38]

☐ La proposition/l'initiative est relative à la **prolongation d'une action existante**

☐ La proposition/l'initiative porte sur une **action réorientée vers une nouvelle action**

### 1.4. Objectifs

*1.4.1. Objectif(s) stratégique(s) pluriannuel(s) de la Commission visé(s) par la proposition/l'initiative*

La directive proposée vise à assurer un niveau commun élevé de sécurité des réseaux et de l'information (SRI) dans toute l'Union.

*1.4.2. Objectifs spécifiques et activités GPA/EBA concernées*

La proposition établit des mesures destinées à assurer un niveau élevé de sécurité commun des réseaux et systèmes d'information dans toute l'Union.

Les objectifs spécifiques sont les suivants:

1. Instaurer un niveau minimum de SRI dans les États membres et donc relever le niveau global de préparation et d'intervention.

2. Améliorer la coopération en matière de SRI au niveau de l'UE en vue de faire face efficacement aux menaces et incidents transnationaux. Une infrastructure sécurisée de partage des informations sera mise en place de manière à permettre l'échange d'informations sensibles et confidentielles entre les autorités compétentes.

[37] GPA: gestion par activité – EBA: établissement du budget par activité.

[38] Tel(le) que visé(e) à l'article 49, paragraphe 6, point a) ou b), du règlement financier.

| |
|---|
| 3. Créer une culture de gestion des risques et améliorer le partage d'informations entre le secteur privé et le secteur public. |

| |
|---|
| Activité(s) ABM/ABB concernée(s)<br><br>La directive concerne des entités (entreprises et organismes, y compris des PME) dans un certain nombre de secteurs (l'énergie, les transports, les établissements de crédit et les bourses de valeurs, les soins de santé et les facilitateurs de services Internet clés) ainsi que des administrations publiques. Elle traite également des relations avec les services répressifs et les autorités chargées de la protection des données ainsi que des aspects des relations extérieures liés à la SRI.<br><br>09 - Réseaux de communication, contenu et technologies<br><br>02 - Entreprises,<br><br>32 - Énergie<br><br>06 - Mobilité et transports<br><br>17 - Santé et protection des consommateurs<br><br>18 – Affaires intérieures<br><br>19 - Relations extérieures<br><br>33 - Justice<br><br>12 - Marché intérieur |

*1.4.3. Résultats et incidences escomptés*

*Préciser les effets que la proposition/l'initiative devrait avoir sur les bénéficiaires/la population visée.*

| |
|---|
| La protection des particuliers, entreprises et pouvoirs publics de l'UE contre les incidents, menaces et risques SRI serait grandement renforcée.<br><br>La partie 8.2 (Impact de l'option 2 – Approche réglementaire) du document de travail des services de la Commission «Analyse d'impact accompagnant la proposition de directive» contient davantage de détails. |

*1.4.4. Indicateurs de résultats et d'incidences*

*Préciser les indicateurs permettant de suivre la réalisation de la proposition/de l'initiative*

| |
|---|
| Les indicateurs pour le suivi et l'évaluation se trouvent à la partie 10 de l'analyse d'impact. |

**1.5. Justification de la proposition/de l'initiative**

*1.5.1. Besoins à satisfaire à court ou à long terme*

| |
|---|
| Chaque État membre serait tenu d'avoir: |

- une stratégie nationale en matière de SRI;

- un plan de coopération en matière de SRI;

- une autorité nationale compétente en matière de SRI; et

- une équipe d'intervention en cas d'urgence informatique (CERT).

Au niveau de l'UE, les États membres seraient tenus de coopérer au sein d'un réseau.

Les administrations publiques et les principaux acteurs privés seraient tenus d'assurer la gestion des risques SRI et de signaler aux autorités compétentes les incidents de SRI ayant un impact significatif.

*1.5.2. Valeur ajoutée de l'intervention de l'UE*

Compte tenu de la dimension transnationale de la SRI, toute divergence dans les législations et politiques applicables constitue un obstacle pour les entreprises opérant dans plusieurs pays et à la réalisation d'économies d'échelle globales. Si l'UE n'intervenait pas, on se retrouverait dans une situation où chaque État membre agit seul sans tenir compte de l'interdépendance entre les réseaux et systèmes informatiques.

Les objectifs énoncés peuvent donc être plus aisément atteints par une action au niveau de l'UE que par les États membres seuls.

*1.5.3. Leçons tirées d'expériences similaires*

La proposition découle du constat selon lequel il est nécessaire d'imposer des obligations réglementaires pour que les règles soient les mêmes partout et que certaines lacunes législatives soient comblées. Dans ce domaine, l'approche strictement volontaire suivie jusqu'à présent a abouti à ce que seule une minorité d'États membres disposant de moyens significatifs coopèrent.

*1.5.4. Compatibilité et synergie éventuelle avec d'autres instruments appropriés*

La proposition est pleinement conforme à la Stratégie numérique pour l'Europe et donc avec la stratégie Europe 2020. Elle est également conforme au cadre réglementaire de l'UE pour les communications électroniques, à la directive de l'UE sur les infrastructures critiques européennes et à la proposition de directive de l'UE sur la protection des données, et les complète.

La proposition accompagne et constitue une partie essentielle de la communication de la Commission et de la haute représentante de l'Union pour les affaires étrangères et la politique de sécurité concernant la stratégie européenne de cybersécurité.

**1.6. Durée et incidence financière**

– ☐ Proposition/initiative à durée limitée

– ☐ Proposition/initiative en vigueur du [JJ/MM]AAAA au [JJ/MM]AAAA

– ☐ Incidence financière de AAAA à AAAA

– ☒ Proposition/initiative à durée illimitée

– Le délai de transposition commencera immédiatement après l'adoption (prévue en 2015) et sera de 18 mois. La mise en œuvre de la directive commencera toutefois dès l'adoption et impliquera de créer l'infrastructure sécurisée sur laquelle reposera la coopération entre États membres.

– Ensuite fonctionnement à plein régime.

### 1.7. Mode de gestion envisagés[39]

– ☒ Gestion centralisée directe par la Commission

– ☒ Gestion centralisée indirecte par délégation de tâches d'exécution à:

– ☐des agences exécutives

– ☒ des organismes créés par les Communautés[40]

– ☐ des organismes publics nationaux/organismes avec mission de service public

– ☐ des personnes chargées de l'exécution d'actions spécifiques en vertu du titre V du traité sur l'Union européenne, identifiées dans l'acte de base concerné au sens de l'article 49 du règlement financier

– ☐ Gestion partagée avec les États membres

– ☐ Gestion décentralisée avec des pays tiers

– ☐ Gestion conjointe avec des organisations internationales, y compris l'Agence spatiale européenne

*Si plusieurs modes de gestion sont indiqués, veuillez donner des précisions dans la partie «Remarques».*

| Remarques:<br><br>L'ENISA, agence décentralisée créée par les Communautés, peut assister les États membres et la Commission dans la mise en œuvre de la directive sur la base de son mandat et par le redéploiement de ressources prévu au titre du CFP 2014-2020 pour cette agence. |
|---|

## 2. MESURES DE GESTION

### 2.1. Dispositions en matière de suivi et de compte rendu

*Préciser la fréquence et les conditions de ces dispositions*

| La Commission réexaminera périodiquement le fonctionnement de la présente directive et en rendra compte au Parlement européen et au Conseil. |
|---|

39 Les explications sur les modes de gestion ainsi que les références au règlement financier sont disponibles sur le site BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_fr.html

40 Tels que visés à l'article 185 du règlement financier.

La Commission établira également si les États membres transposent correctement la directive.

La proposition relative au MIE prévoit également la possibilité de procéder à une évaluation des modalités de réalisation des projets ainsi que de l'incidence de leur mise en œuvre, afin d'apprécier si les objectifs prévus, y compris en matière de protection de l'environnement, ont été atteints.

## 2.2. Système de gestion et de contrôle

### *2.2.1. Risques identifiés*

Retards dans la réalisation du projet en ce qui concerne la mise sur pied de l'infrastructure sécurisée.

### *2.2.2. Moyens de contrôle prévus*

Les accords et décisions de mise en œuvre des actions dans le cadre du MIE prévoiront une supervision et un contrôle financier par la Commission, ou tout représentant autorisé par elle, ainsi que des audits effectués par la Cour des comptes et des contrôles sur place effectués par l'Office européen de lutte antifraude (OLAF).

### *2.2.3. Coûts et avantages des contrôles et taux probable de non-conformité*

Les contrôles *ex ante* et *ex post* fondés sur les risques et la possibilité d'audits sur place permettront de maintenir les coûts du contrôle à un niveau raisonnable.

## 2.3. Mesures de prévention des fraudes et irrégularités

*Préciser les mesures de prévention et de protection existantes ou envisagées.*

La Commission prend les mesures appropriées pour garantir, lors de la mise en œuvre de l'action financée au titre de la présente directive, la protection des intérêts financiers de l'Union par l'application de mesures préventives contre la fraude, la corruption et toute autre activité illégale, par des contrôles efficaces et, si des irrégularités sont décelées, par la récupération des montants indûment versés et, si nécessaire, par des sanctions efficaces, proportionnées et dissuasives.

La Commission ou ses représentants et la Cour des comptes disposent d'un pouvoir d'audit, sur pièces et sur place, à l'égard de tous les bénéficiaires de subventions, contractants et sous-traitants qui ont reçu des fonds de l'Union au titre du présent programme.

L'Office européen de lutte antifraude (OLAF) peut effectuer des contrôles et vérifications sur place auprès des opérateurs économiques concernés, directement ou indirectement, par un tel financement, selon les modalités prévues par le règlement (Euratom, CE) n° 2185/96, en vue d'établir l'existence éventuelle d'une fraude, d'un acte de corruption ou de toute autre activité illégale portant atteinte aux intérêts financiers de l'Union, dans le cadre d'une convention de subvention, d'une décision de subvention ou d'un contrat concernant un financement de l'Union.

Sans préjudice de ce qui précède, les accords de coopération conclus avec des pays tiers et des organisations internationales, les conventions de subvention, les décisions de subvention et les contrats résultant de l'application de la présente directive prévoient expressément que la Commission, la Cour des comptes et l'OLAF sont habilités à procéder à ces audits et ces contrôles et vérifications sur place.

Le MIE prévoit que les contrats, subventions et marchés soient basés sur des modèles standard, lesquels préciseront les mesures antifraude généralement applicables.

## 3. INCIDENCE FINANCIÈRE ESTIMÉE DE LA PROPOSITION/DE L'INITIATIVE

### 3.1. Rubriques du cadre financier pluriannuel et lignes budgétaires de dépenses concernées

- Lignes budgétaires de dépenses existantes

Dans l'ordre des rubriques du cadre financier pluriannuel et des lignes budgétaires.

| Rubrique du cadre financier pluriannuel | Ligne budgétaire | Nature de la dépense | Participation | | | |
|---|---|---|---|---|---|---|
| | Numéro [Description……...…….] | CD/CND [41] | de pays AELE[42] | de pays candidats [43] | de pays tiers | au sens de l'article 18, paragraphe 1, point a) *bis*, du règlement financier |
| | 09 03 02 – Favoriser l'interconnexion et l'interopérabilité des services publics nationaux en ligne ainsi que l'accès à ces réseaux. | Diss. | NON | NON | NON | NON |

- Nouvelles lignes budgétaires dont la création est demandée (sans objet)

*Dans l'ordre des rubriques du cadre financier pluriannuel et des lignes budgétaires.*

| Rubrique du cadre financier pluriannuel | Ligne budgétaire | Nature de la dépense | Participation | | | |
|---|---|---|---|---|---|---|
| | Numéro [Rubrique……..] | CD/CND | de pays AELE | de pays candidats | de pays tiers | au sens de l'article 18, paragraphe 1, point a) *bis*, du règlement financier |
| | [XX.YY.YY.YY] | | OUI/ NON | OUI/NON | OUI/ NON | OUI/NON |

41 CD = crédits dissociés / CND = crédits non dissociés.

42 AELE: Association européenne de libre-échange.

43 Pays candidats et, le cas échéant, pays candidats potentiels des Balkans occidentaux.

### 3.2. Incidence estimée sur les dépenses

*3.2.1. Synthèse de l'incidence estimée sur les dépenses*

En millions d'euros (à la 3e décimale)

| **Rubrique du cadre financier pluriannuel** | 1 | Croissance intelligente et inclusive |
|---|---|---|

| DG: <…….> | | | 2015* [44] | Année **2016** | Année **2017** | Année **2018** | Années suivantes (2019-2021) et ultérieures | | | **TOTAL** |
|---|---|---|---|---|---|---|---|---|---|---|
| • Crédits opérationnels | | | | | | | | | | |
| 09 03 02 | Engagements | (1) | 1,250** | 0,000 | | | | | | **1,250** |
| | Paiements | (2) | 0,750 | 0,250 | 0,250 | | | | | **1,250** |
| Crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques[45] | | | **0,000** | | | | | | | **0,000** |
| Numéro de ligne budgétaire | | (3) | **0,000** | | | | | | | **0,000** |
| **TOTAL des crédits pour la DG** <….> | Engagements | =1+1a +3 | 1,250 | 0,000 | | | | | | **1,250** |
| | Paiements | =2+2a +3 | 0,750 | 0,250 | 0,250 | | | | | **1,250** |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| • TOTAL des crédits opérationnels | Engagements | (4) | 1,250 | 0,000 | | | | | | **1,250** |
| | Paiements | (5) | 0,750 | 0,250 | 0,250 | | | | | **1,250** |
| • TOTAL des crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques | | (6) | **0,000** | | | | | | | |

44 L'année N est l'année du début de la mise en œuvre de la proposition/l'initiative.

45 Assistance technique et/ou administrative et dépenses d'appui à la mise en œuvre de programmes et/ou d'actions de l'UE (anciennes lignes «BA»), recherche indirecte, recherche directe.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **TOTAL des crédits pour la RUBRIQUE 1** du cadre financier pluriannuel | Engagements | =4+6 | 1,250 | 0,000 | | | | | | **1,250** |
| | Paiements | =5+6 | 0,750 | 0,250 | 0,250 | | | | | **1,250** |

* Le calendrier exact dépendra de la date d'adoption de la proposition par l'autorité législative (c.-à-d. que, si la directive était approuvée en 2014, l'adaptation de l'infrastructure existante commencerait en 2015, sinon un an plus tard).

** Si les États membres décident d'utiliser une infrastructure existante et d'imputer le coût unique d'adaptation au budget de l'UE, comme expliqué aux points 1.4.3 et 1.7, le coût d'adaptation d'un réseau pour permettre la coopération entre États membres, conformément au chapitre III de la directive (alerte rapide, intervention coordonnée, etc.) est estimé à 1 250 000 EUR. Ce montant est légèrement supérieur à celui indiqué dans l'analyse d'impact («environ 1 million EUR») car il est calculé à partir d'une estimation plus précise du coût des modules nécessaires à la réalisation d'une telle infrastructure. Les modules nécessaires et les coûts afférents reposent sur une estimation que le CCR a établie grâce à son expérience de l'élaboration de systèmes analogues dans d'autres domaines, comme la santé publique, et comprendraient: un système d'alerte rapide et de notification SRI (275 000 EUR); une plateforme d'échange d'informations (400 000 EUR); un système d'alerte rapide et d'intervention (275 000 EUR); et un centre de crise (300 00 EUR), soit un total de 1 250 000 EUR. Il est prévu d'établir un plan de mise en œuvre plus détaillé dans le cadre de la prochaine étude de faisabilité au titre du contrat spécifique SMART 2012/0010: «Étude de faisabilité et activités préparatoires concernant la réalisation d'un système européen d'alerte rapide et d'intervention en cas de cyberattaques et de perturbations».

**Si plusieurs rubriques sont concernées par la proposition/l'initiative:**

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| • TOTAL des crédits opérationnels | Engagements | (4) | 0,000 | 0,000 | | | | | | |
| | Paiements | (5) | 0,000 | 0,000 | | | | | | |
| • TOTAL des crédits de nature administrative financés par l'enveloppe de certains programmes spécifiques | | (6) | **0,000** | **0,000** | | | | | | |
| **TOTAL des crédits pour les RUBRIQUES 1 à 4** du cadre financier pluriannuel (montant de référence) | Engagements | =4+6 | 1,250 | 0,000 | | | | | | 1,250 |
| | Paiements | =5+6 | 0,750 | 0,250 | 0,250 | | | | | 1,250 |

| **Rubrique du cadre financier pluriannuel** | **5** | «Dépenses administratives» |
|---|---|---|

En millions d'euros (à la 3e décimale)

| | | Année **2015** | Année **2016** | Année **2017** | Année **2018** | Années suivantes (2019-2021) et ultérieures | | | **TOTAL** |
|---|---|---|---|---|---|---|---|---|---|
| DG: CNECT | | | | | | | | | |
| • Ressources humaines | | 0,572 | 0,572 | 0,572 | 0,572 | 0,572 | 0,572 | **0,572** | **4,004** |
| • Autres dépenses administratives | | 0,318 | 0,118 | 0,318 | 0,118 | 0,318 | 0,118 | **0,118** | **1,426** |
| **TOTAL DG** CNECT | Crédits | 0,890 | 0,690 | 0,890 | 0,690 | 0,890 | 0,690 | 0,690 | **5,430** |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **TOTAL des crédits pour la RUBRIQUE 5** du cadre financier pluriannuel | (Total des engagements = Total des paiements) | 0,890 | 0,690 | 0,890 | 0,690 | 0,890 | 0,690 | 0,690 | **5,430** |

En millions d'euros (à la 3e décimale)

| | | Année **2015**[46] | Année **2016** | Année **2017** | Année **2018** | Années suivantes (2019-2021) et ultérieures | | | **TOTAL** |
|---|---|---|---|---|---|---|---|---|---|
| **TOTAL des crédits pour les RUBRIQUES 1 à 5** du cadre financier pluriannuel | Engagements | 2,140 | 0,690 | 0,890 | 0,690 | 0,890 | 0,690 | 0,690 | **6,680** |
| | Paiements | 1,640 | 0,940 | 1,140 | 0,690 | 0,890 | 0,690 | 0,690 | **6,680** |

[46] L'année N est l'année du début de la mise en œuvre de la proposition/l'initiative.

*3.2.2. Incidence estimée sur les crédits opérationnels*

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits opérationnels.

– ☑ La proposition/l'initiative engendre l'utilisation de crédits opérationnels, comme expliqué ci-après:

– Crédits d'engagement en millions d'euros (à la 3e décimale)

| **Indiquer les objectifs et les réalisations** ⇩ | | | Année **2015*** | | Année **2016** | | Année **2017** | | Année **2018** | | Années suivantes (2019-2021) et ultérieures | | | | | | **TOTAL** | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | **RÉALISATIONS** | | | | | | | | | | | | | | | |
| | Type[47] | Coût moyen | Nombre | Coût | Nombre | Coût | Nombre | Coût | Nombre | Coût | Nombre | Coût | Nombre | Coût | Nombre | Coût | Nombre total | Coût total |
| OBJECTIF SPÉCIFIQUE N° 2[48]<br>Infrastructure sécurisée d'échange d'informations | | | | | | | | | | | | | | | | | | |
| - Réalisation | Adaptation de l'infrastructur | | | | | | | | | | | | | | | | | |
| Sous-total pour l'objectif spécifique n° 2 | | | 1 | 1,250** | | | | | | | | | | | | | 1 | 1,250 |
| **COÛT TOTAL** | | | | 1,250 | | | | | | | | | | | | | | 1,250 |

* Le calendrier exact dépendra de la date d'adoption de la proposition par l'autorité législative (c.-à-d. que, si la directive était approuvée en 2014, l'adaptation de l'infrastructure existante commencerait en 2015, sinon un an plus tard).

47 On entend par «réalisations» les produits et services à fournir (nombre d'échanges d'étudiants financés, nombre de kilomètres de route construits, etc.).

48 Tel que décrit à la partie 1.4.2. «Objectif(s) spécifique(s)…».

** Voir point 3.2.1.

*3.2.3. Incidence estimée sur les crédits de nature administrative*

3.2.3.1. Synthèse

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de crédits de nature administrative.

– ☑ La proposition/l'initiative engendre l'utilisation de crédits de nature administrative, comme expliqué ci-après:

En millions d'euros (à la 3e décimale)

| | Année **2015**[49] | Année **2016** | Année **2017** | Année **2018** | Années suivantes (2019-2021) et ultérieures | | | **TOTAL** |
|---|---|---|---|---|---|---|---|---|
| **RUBRIQUE 5 du cadre financier pluriannuel** | | | | | | | | |
| Ressources humaines | 0,572 | 0,572 | 0,572 | 0,572 | 0,572 | 0,572 | 0,572 | **4,004** |
| Autres dépenses administratives | 0,318 | 0,118 | 0,318 | 0,118 | 0,318 | 0,118 | 0,118 | **1,426** |
| **Sous-total de la RUBRIQUE 5 du cadre financier pluriannuel** | 0,890 | 0,690 | 0,890 | 0,690 | 0,890 | 0,690 | 0,690 | **5,430** |
| **Hors RUBRIQUE 5**[50] **du cadre financier pluriannuel** | | | | | | | | |
| Ressources humaines | 0,000 | 0,000 | | | | | | **0,000** |
| Autres dépenses de nature administrative | | | | | | | | |
| **Sous-total hors RUBRIQUE 5 du cadre financier pluriannuel** | 0,890 | 0,690 | 0,890 | 0,690 | 0,890 | 0,690 | 0,690 | **5,430** |
| **TOTAL** | 0,890 | 0,690 | 0,890 | 0,690 | 0,890 | 0,690 | 0,690 | **5,430** |

Les besoins en crédits de nature administrative seront couverts par les dotations de la DG CNECT qui sont déjà affectées à la gestion de l'action et/ou qui sont redéployées au sein de la DG, complétées le cas échéant par toute dotation additionnelle qui pourrait être allouée à la

49 L'année N est l'année du début de la mise en œuvre de la proposition/l'initiative.

50 Assistance technique et/ou administrative et dépenses d'appui à la mise en œuvre de programmes et/ou d'actions de l'UE (anciennes lignes «BA»), recherche indirecte, recherche directe.

DG gestionnaire dans le cadre de la procédure d'allocation annuelle et à la lumière des contraintes budgétaires.

L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) pourrait assister les États membres et la Commission dans la mise en œuvre de la directive sur la base de son mandat et par le redéploiement de ressources prévu au titre du CFP 2014-2020 pour cette agence, c.-à-d. sans dotation additionnelle en ressources financières ou humaines.

3.2.3.2. Besoins estimés en ressources humaines

– ☐ La proposition/l'initiative n'engendre pas l'utilisation de ressources humaines.

– ☑ La proposition/l'initiative engendre l'utilisation de ressources humaines de la Commission, comme expliqué ci-après:

En principe, aucune main-d'œuvre supplémentaire ne devrait être nécessaire. Les ressources humaines requises seront très limitées et seront fournies par le personnel de la DG qui est déjà affecté à la gestion de l'action.

*Estimation à exprimer en valeur entière (ou au plus avec une décimale)*

| | | Année **2015** | Année **2016** | Année **2017** | Année **2018** | Années suivantes (2019-2021) et ultérieures | | |
|---|---|---|---|---|---|---|---|---|
| **• Emplois du tableau des effectifs (postes de fonctionnaires et d'agents temporaires)** | | | | | | | | |
| 09 01 01 01 (au siège et dans les bureaux de représentation de la Commission) | | 4 | 4 | 4 | 4 | 4 | 4 | 4 |
| XX 01 01 02 (en délégation) | | | | | | | | |
| XX 01 05 01 (recherche indirecte) | | | | | | | | |
| 10 01 05 01 (recherche directe) | | | | | | | | |
| **• Personnel externe (en équivalent temps plein: ETP)**[51] | | | | | | | | |
| 09 01 02 01 (AC, INT, END sur l'enveloppe globale) | | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| XX 01 02 02 (AC, INT, JED, AL et END dans les délégations) | | | | | | | | |
| **XX** 01 04 **yy** [52] | - au siège[53] | | | | | | | |
| | - en délégation | | | | | | | |
| **XX** 01 05 02 (AC, INT, END sur recherche indirecte) | | | | | | | | |
| 10 01 05 02 (AC, INT, END sur recherche directe) | | | | | | | | |
| Autre ligne budgétaire (à préciser) | | | | | | | | |
| **TOTAL** | | **5** | **5** | **5** | **5** | **5** | **5** | **5** |

**XX** est le domaine politique ou le titre concerné.

Les besoins en ressources humaines seront couverts par les effectifs de la DG CNECT déjà affectés à la gestion de l'action et/ou redéployés en interne au sein de la DG, complétés le cas échéant par toute dotation additionnelle qui pourrait être allouée à la DG gestionnaire dans le cadre de la procédure d'allocation annuelle et à la lumière des contraintes budgétaires.

51 AC = agent contractuel; INT = intérimaire; JED = jeune expert en délégation; AL = agent local; END = expert national détaché.

52 Sous-plafond de personnel externe sur crédits opérationnels (anciennes lignes «BA»).

53 Essentiellement pour les Fonds structurels, le Fonds européen agricole pour le développement rural (Feader) et le Fonds européen pour la pêche (FEP).

L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) pourrait assister les États membres et la Commission dans la mise en œuvre de la directive sur la base de son mandat actuel et par le redéploiement de ressources prévu au titre du CFP 2014-2020 pour cette agence, c.-à-d. sans dotation additionnelle en ressources financières ou humaines.

Description des tâches à effectuer:

| | |
|---|---|
| Fonctionnaires et agents temporaires | - Préparation d'actes délégués conformément à l'article 14, paragraphe 3.<br><br>- Préparation d'actes d'exécution conformément à l'article 8, l'article 9, paragraphe 2, l'article 12, l'article 14, paragraphe 5, et l'article 16.<br><br>- Contribution à la coopération par le réseau, au niveau politique et opérationnel.<br><br>- Participation à des négociations internationales et conclusion éventuelle d'accords internationaux. |
| Personnel externe | Participation aux tâches ci-dessus en fonction des besoins. |

*3.2.4. Compatibilité avec le cadre financier pluriannuel actuel*

– ☑ La proposition/l'initiative est compatible avec le cadre financier pluriannuel actuel.

– ☐ La proposition/l'initiative nécessite une reprogrammation de la rubrique concernée du cadre financier pluriannuel.

L'incidence financière estimée de la proposition sur les dépenses opérationnelles sera subie si les États membres décident d'adapter une infrastructure existante et chargent la Commission de mettre en œuvre l'adaptation au titre du CFP 2014-2020. Le coût unique correspondant serait couvert au titre du MIE à condition que des fonds suffisants soient disponibles. Sinon, les États membres peuvent partager soit les coûts d'adaptation de l'infrastructure soit les coûts de création d'une nouvelle infrastructure.

– ☐ La proposition/l'initiative nécessite le recours à l'instrument de flexibilité ou la révision du cadre financier pluriannuel[54].

Sans objet.

*3.2.5. Participation de tiers au financement*

– La proposition/l'initiative ne prévoit pas de cofinancement par des tierces parties.

**3.3. Incidence estimée sur les recettes**

– ☑ La proposition/l'initiative est sans incidence financière sur les recettes.

[54] Voir points 19 et 24 de l'accord interinstitutionnel.