N° 7314[5]

CHAMBRE DES DEPUTES

Session ordinaire 2018-2019

P R O J E T D E L O I

portant transposition de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union européenne et modifiant

1° la loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'Information de l'Etat et

2° la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale

* * *

AVIS DE LA CHAMBRE DE COMMERCE

sur le projet de loi et les amendements gouvernementaux y relatifs

(14.11.2018)

Le projet de loi sous avis (ci-après le « Projet ») a pour objet de transposer en droit national la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (ci-après la « Directive NIS »)[1]. Suite à la publication d'un premier avis du Conseil d'État sur le Projet[2], des amendements gouvernementaux ont été déposés le 2 octobre 2018. En l'absence de saisine formelle du Ministre d'Etat portant sur les amendements au Projet, le présent avis de la Chambre de Commerce porte également sur les amendements.

L'adoption de la Directive NIS doit être analysée dans le contexte de l'augmentation des menaces et des défis cybernétiques qui accompagnent la numérisation de la société[3]. Elle vise à harmoniser les approches entre États membres en établissant des exigences minimales communes en matière de planification, de coopération, ainsi qu'en matière de sécurité pour les opérateurs de services essentiels (ci-après « OSE »)[4] et pour les fournisseurs de services numériques (ci-après « FSN »)[5]. Le Projet porte principalement sur les trois domaines suivants :

– **la gestion des risques**, qui passe par l'établissement d'exigences en matière de sécurité et de notification à charge des OSE et des FSN. Conformément aux dispositions de la Directive NIS, le Projet

---

1 La directive (UE) 2016/1148 est communément appelée « Directive NIS » en raison de son intitulé anglais « Directive on Security of Network and Information Systems ».

2 Avis 52.854 du Conseil d'Etat du 10 juillet 2018, disponible en ligne : https://conseil-etat.public.lu/fr/avis/2018/iuillet2018/10072018/52854.html

3 Voir, dans ce sens, la Communication de la Commission au Parlement européen et au Conseil, « *Exploiter tout le potentiel de la directive SRI – Vers la mise en oeuvre effective de la directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union* », COM (2017) 476 final du 4 octobre 2017.

4 En application du chapitre 3 du Projet, un OSE est une entité qui fournit un service tributaire des réseaux et systèmes d'information qui est essentiel au maintien d'activités sociétales et/ou économiques critiques, et sur la fourniture duquel un incident aurait un effet disruptif important. En application de l'article 5 de la Directive NIS, les OSE doivent être identifiés au niveau national pour chaque secteur concerné au plus tard le 9 novembre 2018. Pour ce faire, l'article 7 du Projet détermine les critères d'identification et les secteurs concernés sont définis dans l'annexe.

5 Ne sont pas visés par le Projet les FNS remplissant les critères de la micro et de la petite entreprise au sens de la recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micros, petites et moyennes entreprises.

prévoit qu'il appartient aux OSE, ainsi que, dans une moindre mesure, aux FSN, de prendre les mesures techniques et organisationnelles nécessaires et proportionnées pour gérer les risques et pour prévenir, sinon limiter, l'impact des incidents qui compromettent la sécurité des réseaux et des systèmes d'information ;

– **la détermination des défis cybernétiques**, tâche qui incombe aux États membres et qui passe notamment par la désignation d'autorités nationales compétentes, et par l'adoption d'une stratégie nationale en matière de sécurité des réseaux et des systèmes d'informations[6]. La Commission de Surveillance du Secteur Financier (ci-après « CSSF ») et l'Institut luxembourgeois de régulation (ci-après « ILR »)[7] sont les autorités nationales compétentes en vertu du Projet ; et
– **le renforcement de la coopération et l'échange d'informations** entre les États membres et les diverses entités compétentes.

*

CONSIDERATIONS GENERALES

De manière générale, la Chambre de Commerce souhaite mettre en lumière la complexification croissante de la règlementation entourant l'activité des opérateurs économiques impliqués dans le fonctionnement des réseaux et des infrastructures au niveau national. En effet, il est très probable que des opérateurs déjà concernés par la législation relative aux infrastructures critiques au sens de la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la protection nationale[8] soient également soumis au Projet sous avis en leur qualité d'OSE. Dans un monde où les interconnexions sont croissantes, une telle règlementation est nécessaire, cependant la Chambre de Commerce souhaite rappeler qu'il ne faut pas minimiser son impact, notamment financier, sur les opérateurs des secteurs concernés.

En ce qui concerne les dispositions précises du Projet, la Chambre de Commerce rappelle l'importance du principe de **transposition fidèle des directives européennes**. En effet, le respect de ce principe « *toute la directive, rien que la directive* » vise à garantir que les entreprises luxembourgeoises ne soient pas confrontées à des règles plus strictes que celles appliquées dans les autres Etats membres. Or, contrairement aux indications fournies au point 10 de la fiche d'évaluation d'impact, plusieurs dispositions du Projet imposent des obligations qui ne sont pas prévues par la Directive NIS.

La Chambre de Commerce souhaite notamment mettre en évidence les risques engendrés, pour les opérateurs, par l'ajout de cas où l'autorité compétente décide de **porter à la connaissance du public un incident notifié**[9]. Alors que la Directive NIS prévoit que l'autorité compétente concernée « *peut informer le public concernant des incidents particuliers, lorsque la sensibilisation du public est nécessaire pour prévenir un incident ou gérer un incident en cours* »[10], l'article 8, paragraphe 8 du Projet y ajoute le cas suivant : « *ou lorsque la divulgation de l'incident est dans l'intérêt du public à d'autres égards* »[11]. Dans la mesure où ceci ne résulte pas du texte de la directive à transposer, la Chambre de

---

6 La mission de coordination et d'élaboration de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information est confiée au Haut-Commissariat à la protection nationale. Cette compétence étant relative aux mesures d'anticipation de crises, le projet d'article 16 vise à l'intégrer à l'article 3, paragraphe 1er, point b) de la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale.

En outre, le Projet vise également à transférer la fonction d'Autorité d'agrément cryptographique, exercée jusqu'à présent par l'Agence nationale de la sécurité des services d'information (ANSSI), au Centre des technologies de l'information de l'Etat (CTIE).

7 L'ILR est également désigné comme point de contact national unique exerçant une fonction de liaison pour assurer une coopération transfrontalière (projet d'article 4).

8 En vertu de l'article 2 de la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection Nationale, est une infrastructure critique « t*out point, système ou partie de celui-ci qui est indispensable à la sauvegarde des intérêts vitaux ou des besoins essentiels de tout ou partie du pays ou de la population ou qui est susceptible de faire l'objet d'une menace particulière* ».

9 Projet d'article 8, paragraphe 8 concernant les incidents notifiés par un OSE.

10 Directive NIS, article 14, paragraphe 6

11 Le projet d'article prévoit également la possibilité pour l'autorité compétente d'imposer à l'opérateur concerné d'informer lui-même le public.

Commerce demande, afin d'éviter tout risque pour les opérateurs luxembourgeois, notamment en matière d'image et sur le plan commercial, de s'en tenir à une transposition du texte de la Directive[12].

La Chambre de Commerce relève également que, dans les cas où la sécurité des réseaux et des systèmes d'informations implique également des données personnelles, il existe un risque de **dédoublement des procédures** entre d'une part celles mises en place dans le Projet, et d'autre part celles applicables en vertu du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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 (ci-après le « RGPD »). Ce constat porte à la fois sur l'**obligation d'identification des risques**[13], et sur la procédure de **notification de tout incident à l'autorité compétente**[14]. Dans ce dernier cas, la Chambre de Commerce relève qu'un tel dédoublement des notifications est susceptible d'engendrer une lourdeur administrative importante pour les opérateurs contraints de répondre dans l'urgence aux exigences des autorités administratives compétentes en vertu des différents textes légaux.

Quant à la forme ensuite, et avant toute analyse du détail des articles du Projet, la Chambre de Commerce regrette que le Projet lui ait été soumis après l'**écoulement du délai de transposition**[15], l'empêchant de soumettre le Projet à une analyse aussi approfondie que ce sujet l'aurait mérité.

Elle regrette également que les projets de règlements grand-ducaux d'exécution du Projet sous avis ne lui aient pas été communiqués en même temps que le Projet, lui permettant ainsi de procéder à une analyse complète du système mis en place.

En ce qui concerne la **fiche financière**, elle ne peut que constater son caractère éminemment succinct, cette dernière se limitant une liste des frais supplémentaires, sans aucunes projections financières. Malgré une remarque du Conseil d'Etat dans ce sens[16], aucun complément d'information n'a été communiqué afin de compléter la fiche financière pour la rendre conforme aux exigences de l'article 79 de la loi modifiée du 8 juin 1999 sur le budget, la compatibilité et la trésorerie de l'État[17].

*

COMMENTAIRE DES ARTICLES

Article 8 du Projet[18]

L'article 8 du Projet détaille l'ensemble des obligations qui pèsent sur les OSE, y compris notamment l'identification des risques, la prévention des incidents, ou encore la notification des incidents et les relations de l'OSE avec l'autorité compétente.

La Chambre de Commerce note à la lecture du commentaire de l'article sous analyse que « *les régulateurs entendent profiter de la période courant jusqu'à l'adoption du présent projet de loi afin*

---

12 Voir le commentaire de l'article 8 du Projet ci-dessous.

13 „Alors que les **articles 8, paragraphe 1er et 11, paragraphe 1er du Projet** imposent aux OSE et aux FSN d'identifier « *les risques qui menacent la sécurité des réseaux et des systèmes d'information […] et prennent les mesures techniques et organisationnelles nécessaires et proportionnées pour les gérer* », **l'article 32 du RGPD** prévoit que « *Compte tenu de l'état des connaissances, des coûts de mise en oeuvre […] le responsable du traitement et le sous-traitant mettent en oeuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque […]* ».

14 „Alors que **l'article 8, paragraphe 4 du Projet** prévoit que « *les OSE notifient à l'autorité compétente concernée, sans retard injustifié, les incidents qui ont un impact significatif sur la continuité des services essentiels qu'ils fournissent* » (l'article 11, paragraphe 3 impose la même obligation aux FSN pour tout incident ayant un impact significatif sur la fourniture d'un service numérique qu'ils offrent), **l'article 33, paragraphe 1er du RGPD** prévoit que « *En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente […] dans les meilleurs délais* ».

15 En vertu de l'article 25 de la Directive NIS, les Etats membres devaient transposer la directive en droit national au plus tard le 9 mai 2018.

16 Avis du Conseil d'Etat n°52.854 du 10 juillet 2018, p.2.

17 L'article 79 de la loi modifiée du 8 juin 1999 sur le budget, la compatibilité et la trésorerie de l'État prévoit que : « *(1) Lorsque des projets ou propositions de loi […] comportent des dispositions dont l'application est susceptible de grever le budget, ils sont obligatoirement accompagnés d'un exposé des recettes et des dépenses nouvelles ou des modifications de recettes et de dépenses à prévoir au budget. Cet exposé comprend une fiche financière [qui] doit comporter tous les renseignements permettant d'identifier la nature et ta durée des dépenses proposées, leur impact sur les dépenses de fonctionnement et de personnel.* »

18 La numérotation correspond à la version amendée du Projet.

d'examiner la possibilité de mettre en place une plateforme de notification unique »[19]. Elle soutient une telle initiative qui constituerait une mesure de simplification administrative bienvenue pour les opérateurs concernés. La Chambre de Commerce engage d'ailleurs les auteurs à préciser le Projet sur ce point.

La Chambre de Commerce constate ensuite que, contrairement aux obligations découlant de la Directive NIS, le paragraphe 3 du projet d'article 8 vise à imposer aux OSE une **charge supplémentaire de notification** à l'autorité compétente **de toutes les mesures prises en matière de gestion de risques ou de prévention des incidents**. La Chambre de Commerce rappelle son attachement au principe de transposition de « *toute la directive, rien que la directive* » et invite les auteurs à s'assurer de la nécessité d'une telle obligation supplémentaire à charge des opérateurs.

Le paragraphe 8 de l'article sous analyse concerne quant à lui la procédure d'information du public en cas d'incident. Comme évoqué ci-avant, son contenu s'éloigne également de celui de la Directive NIS et constitue un risque potentiellement important pour les OSE, notamment en matière d'image et sur le plan commercial. Il accorde notamment aux autorités compétentes le pouvoir :

– d'imposer aux OSE d'informer eux-mêmes le public d'incidents ayant fait l'objet d'une notification ;
– d'informer le public d'incidents particuliers dans le cas où « *la divulgation de l'incident est dans l'intérêt du public à d'autres égards* ».

Aussi, la Chambre de Commerce suggère de s'en tenir à une transposition du texte de la Directive et que l'article sous analyse soit reformulé comme suit :

« *(8) Après avoir consulté l'opérateur de services essentiels qui est à l'origine de la notification, l'autorité compétente concernée peut informer le public d'incidents particuliers ~~ou imposer à l'opérateur de services essentiels de le faire~~, lorsque la sensibilisation du public est nécessaire pour prévenir un incident ou gérer un incident en cours~~, ou lorsque la divulgation de l'incident est dans l'intérêt public à d'autres égards~~* ».

*

Après consultation de ses ressortissants, la Chambre de Commerce est en mesure d'approuver le projet de loi sous avis sous réserve de la prise en considération de ses commentaires.

19 Commentaire des articles, p. 34