# N° 7670

## CHAMBRE DES DEPUTES

Session ordinaire 2019-2020

# P R O J E T  D E  L O I

**modifiant**

**1° la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale,**

**2° la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'Etat,**

**3° la loi modifiée du 27 février 2011 sur les réseaux et les services de communications électroniques,**

**4° la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat et**

**5° la loi modifiée du 8 avril 2018 sur les marchés publics**

* * *

*(Dépôt: le 15.9.2020)*

**SOMMAIRE:**



*

## ARRETE GRAND-DUCAL DE DEPOT

Nous HENRI, Grand-Duc de Luxembourg, Duc de Nassau,

Sur le rapport de Notre Premier ministre, ministre d'État et après délibération du Gouvernement en Conseil ;

Arrêtons :

*Article unique.* – Notre Premier ministre, ministre d'État est autorisé à déposer en Notre nom à la Chambre des Députés le projet de loi modifiant

1° la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale,

2° la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'État,

3° la loi modifiée du 27 février 2011 sur les réseaux et les services de communications électroniques,

4° la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État et

5° la loi modifiée du 8 avril 2018 sur les marchés publics.

Cabasson, le 29 juillet 2020

*Le Premier ministre,*
*ministre d'État,*
Xavier BETTEL

HENRI

*

## TEXTE DU PROJET DE LOI

**Art. I^er^.** La loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale est modifiée comme suit :

1° L'article 2, point 4, est remplacé par le texte suivant :

« « infrastructure critique » : tout 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 ; » ;

2° À l'article 2, il est inséré un point 4*bis* libellé comme suit :

« 4*bis*. « sécurité de l'information » : sécurité autour des réseaux et systèmes d'information non classifiés installés et exploités par les administrations et services de l'État ; » ;

3° À l'article 3, il est inséré un paragraphe 1*bis* libellé comme suit :

« (1*bis*) Le Haut-Commissariat à la Protection nationale assure les fonctions d'Agence nationale de la sécurité des systèmes d'information, ci-après « ANSSI », de Centre de traitement des urgences informatiques, ci-après « CERT Gouvernemental » et de Service de la communication de crise. » ;

4° Sont insérés à la suite de l'article 9*bis*, les nouveaux chapitres 4*ter*, 4*quater* et 4*quinquies* qui prennent la teneur suivante :

**« Chapitre 4*ter* – L'Agence nationale de la sécurité des systèmes d'information**

**Art. 9*ter*.** (1) Dans sa fonction d'ANSSI, le Haut-Commissariat à la Protection nationale a pour missions :

a) de définir la politique générale de sécurité de l'information de l'État ;

b) de définir, en concertation avec les administrations et services de l'État, les politiques et lignes directrices de sécurité de l'information pour les domaines spécifiques, d'émettre des recomman-

dations d'implémentation y relatives et d'assister les entités au niveau de l'implémentation des mesures proposées ;

c) de définir, en concertation avec les administrations et services de l'État, une approche de gestion des risques, en vue de constituer un plan d'évaluation et d'identification des risques concernant la sécurité de l'information et d'accompagner, à leur demande, les entités dans l'analyse et la gestion des risques ;

d) de conseiller l'Institut national d'administration publique, respectivement, à leur demande, les administrations et services de l'État dans la définition d'un programme de formation dans le domaine de la sécurité de l'information ;

e) de promouvoir la sécurité de l'information par le biais de mesures de sensibilisation ;

f) d'assurer la fonction d'autorité TEMPEST en veillant à la conformité des réseaux et systèmes d'information classifiés aux stratégies et lignes directrices TEMPEST et en approuvant les contre-mesures TEMPEST pour les installations et les produits destinés à protéger des pièces classifiées jusqu'à un certain niveau de classification dans leur environnement opérationnel.

(2) Les missions de l'ANSSI peuvent être élargies, à leur demande, à d'autres autorités publiques, aux établissements publics, ainsi qu'aux infrastructures critiques.

### Chapitre 4*quater* – Le CERT Gouvernemental

**Art. 9*quater*.** (1) Dans sa fonction de CERT Gouvernemental, le Haut-Commissariat à la Protection nationale a pour missions :

a) de constituer le point de contact unique dédié au traitement des incidents de sécurité d'envergure affectant les réseaux et les systèmes d'information des administrations et services de l'État ;

b) d'assurer un service de veille, de détection, d'alerte et de réaction aux attaques informatiques et aux incidents de sécurité d'envergure affectant ces réseaux et systèmes d'information ;

c) d'assurer la fonction de centre national de traitement des urgences informatiques, dénommé CERT National, en

   1. opérant comme le point de contact officiel national pour les CERTs nationaux et gouvernementaux étrangers ;
   2. opérant comme le point de contact officiel national pour la collecte et la distribution d'informations relatives aux incidents de sécurité qui concernent les réseaux et systèmes d'information implantés au Luxembourg ;
   3. relayant les informations collectées aux CERTs sectoriels en charge de la cible d'une attaque ou à défaut de CERT sectoriel, directement à la cible.

d) d'assurer la fonction de centre militaire de traitement des urgences informatiques, dénommé CERT Militaire, en

   1. opérant comme le point de contact officiel national pour les CERTs militaires étrangers ;
   2. assurant un service de veille, de détection, d'alerte et de réaction aux attaques informatiques et aux incidents de sécurité d'envergure affectant les réseaux et les systèmes de communication et de traitement de l'information de l'armée à partir du territoire du Grand-Duché ;
   3. opérant, à partir du territoire du Grand-Duché, une équipe d'intervention spécialisée capable de prendre en charge la réponse aux incidents de sécurité d'envergure liés à ces systèmes de communication et de traitement de l'information.

(2) Les missions du CERT Gouvernemental peuvent être élargies, à leur demande, à d'autres autorités publiques, aux établissements publics, ainsi qu'aux infrastructures critiques.

(3) Pour l'exécution de ses missions, le CERT Gouvernemental bénéficie de la part des administrations et services de l'État de toute la collaboration nécessaire.

### Chapitre 4*quinquies* – Le Service de la communication de crise

**Art. 9*quinquies*.** Dans sa fonction de Service de la communication de crise, le Haut-Commissariat à la Protection nationale a pour missions :

a) de coordonner la communication de crise avant, pendant et après des situations de crise pouvant frapper le territoire national, par l'intermédiaire des médias, l'internet et les réseaux sociaux ;

b) d'effectuer une communication préventive et pédagogique en sensibilisant les médias et le public sur les questions relevant de la protection du pays, de ses sites sensibles et de sa population ;

c) de créer et de maintenir des contacts étroits et réguliers avec les services de communication de crise étrangers. » ;

5° À l'article 10 sont apportées les modifications suivantes :

a) à l'alinéa 1er, les termes « à la fonction de Haut-Commissaire à la Protection nationale » sont remplacés par ces de « aux fonctions de Haut-Commissaire à la Protection nationale et de Haut-Commissaire à la Protection nationale adjoint » ;

b) l'alinéa 2 est complété comme suit :

« Il est assisté d'un Haut-Commissaire à la Protection nationale adjoint auquel il peut déléguer certaines de ses attributions et qui le remplace en cas d'absence. » ;

6° À l'article 11 sont apportées les modifications suivantes :

a) au paragraphe 1er, les termes « , un Haut-Commissaire à la Protection nationale adjoint » sont insérés entre les termes « Haut-Commissaire à la Protection nationale » et « et des fonctionnaires » ;

b) le paragraphe 2, alinéa 2, est supprimé ;

7° Il est inséré à la suite de l'article 15, un article 15*bis* qui prend la teneur suivante :

« **Art. 15*bis*.** (1) Le personnel de l'ANSSI, du CERT Gouvernemental et du SCC est repris dans le cadre du personnel du Haut-Commissariat à la Protection nationale.

(2) Les fonctionnaires disposant d'un grade de substitution ou d'une majoration d'échelon pour postes à responsabilités particulières avant la reprise continuent à en bénéficier par dépassement du nombre limite fixé en vertu des dispositions de l'article 16 de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État aussi longtemps qu'ils restent titulaires d'un poste à responsabilités particulières. Il en est de même des employés qui bénéficient d'une telle majoration sur la base de l'article 29 de la loi modifiée du 25 mars 2015 déterminant le régime et les indemnités des employés de l'État. » ;

**Art. II.** L'article 1er, alinéa 2, quatorzième tiret, de la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'État est remplacé par le tiret suivant :

« – de Haut-Commissaire à la Protection nationale et de Haut-Commissaire à la Protection nationale adjoint, ».

**Art. III.** L'article 5 de la loi modifiée du 27 février 2011 sur les réseaux et les services de communications électroniques est modifié comme suit :

1° Au paragraphe 1er, les termes « de crise internationale grave ou de catastrophe » sont remplacés par ceux de « de crise internationale grave, de catastrophe ou de crise au sens de la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale » ;

2° Au paragraphe 2, les termes « de catastrophe majeure » sont remplacés par ceux de « de catastrophe majeure ou de crise au sens de la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale ».

**Art. IV.** La loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État est modifiée comme suit :

1° A l'article 12, paragraphe 1er, alinéa 7, point 8°, les termes « de Haut-Commissaire à la Protection nationale adjoint » sont ajoutés devant les termes « et de vice-président » ;

2° A l'article 17, lettre b), les termes « Haut-Commissaire à la Protection nationale adjoint » sont insérés après les termes « Haut-Commissaire à la Protection nationale, » ;

3° L'article 22 est complété par le paragraphe suivant :

« (10) Une prime d'astreinte d'une valeur de 12 points indiciaires peut être allouée au personnel du Haut-Commissariat à la Protection nationale soumis à une obligation de permanence ou de pré-

sence. Cette prime est attribuée par décision du ministre du ressort et sur proposition du Haut-Commissaire à la Protection nationale. » ;

4° A l'annexe B2) Allongements, au point 1, les termes « , de Haut-Commissaire à la Protection nationale adjoint » sont ajoutés devant les termes « ou de vice-président ».

**Art. V.** La loi modifiée du 8 avril 2018 sur les marchés publics est modifiée comme suit :

1° A l'article 20, paragraphe 1er, lettre m), le tiret suivant est inséré entre les deuxième et troisième tirets :

« – pour les travaux de réfection de dommages résultant d'une crise telle que définie à l'article 2, point 2, de la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, et pour autant que la réparation soit urgente ; » ;

2° L'article 159, paragraphe 3, est complété par l'alinéa suivant :

« En cas de survenance d'une crise telle que définie à l'article 2, point 2, de la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, le Haut-Commissariat à la Protection nationale est exempté du respect de l'obligation visée à l'alinéa qui précède, pour la passation de marchés en application des articles 20, paragraphe 1er, lettre f), 64, paragraphe 2, lettre c), et 124, lettre d), dès lors que les conditions d'application de ces dispositions sont remplies. ».

*

## EXPOSE DES MOTIFS

Le projet de loi a pour principal objet d'adapter la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale afin de confier à ce dernier, en ligne avec une recommandation formulée par le Conseil d'État, différentes fonctions en matière d'anticipation, de prévention et de gestion des crises, et plus précisément au niveau de la sécurité de l'information d'une part et du traitement des incidents de sécurité d'autre part. Ces fonctions sont exercées par des services créés sur base de différents arrêtés grand-ducaux. Il y a lieu de noter que les services en question, à savoir l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et le Centre de traitement des urgences informatiques (CERT Gouvernemental) exercent leurs missions déjà aujourd'hui sous la responsabilité du Haut-Commissariat à la Protection nationale (HCPN). La même approche est proposée pour le Service de la communication de crise (SCC) qui fonctionne également sous la responsabilité du Haut-Commissariat. A travers cette démarche, les auteurs du projet de loi entendent conférer une base juridique solide à l'exercice des fonctions précitées.

Ensuite, le projet de loi limite la définition de l'infrastructure critique, en vue de l'aligner avec l'interprétation et l'application qui en a été faite au cours des dernières années.

En outre, il est proposé de procéder à travers le présent projet de loi à des ajustements ponctuels de deux textes législatifs, afin de les aligner sur la terminologie et les missions décrites dans la loi portant création d'un Haut-Commissariat à la Protection nationale. D'une part, les termes employés dans la loi modifiée du 27 février 2011 sur les réseaux et les services de communications électroniques sont adaptés afin d'assurer que les mesures exceptionnelles de réquisition et d'interdiction qui y sont inscrites puissent être mises en œuvre en présence d'une crise nationale telle que définie dans la loi portant création d'un Haut-Commissariat à la Protection nationale. D'autre part, la gestion des situations de crise résultant des intempéries qui avaient frappé les régions de l'Ernztal en 2016 et du Mullerthal en 2018 et la lutte contre la propagation du COVID-19 ont montré la nécessité d'adapter la loi modifiée du 8 avril 2018 sur les marchés publics afin de permettre aux autorités étatiques de recourir, dans une situation d'urgence, à une procédure simplifiée de passation des marchés.

Enfin, la nouvelle loi apporte des modifications en matière de personnel du HCPN. D'abord, il est profité du présent projet de loi pour tenir compte de l'évolution que le Haut-Commissariat a connue au cours des dernières années tant du côté de ses missions que du côté de l'évolution du personnel pour créer la fonction de Haut-Commissaire à la Protection nationale adjoint. Ensuite, le projet attribue une prime d'astreinte d'une valeur de 12 points indiciaires au personnel du Haut-Commissariat soumis à une obligation de permanence ou de présence.

### 1. Attribution au HCPN des fonctions d'Agence nationale de la sécurité des systèmes d'information, de Centre de traitement des urgences informatiques et de Service de la communication de crise

Comme indiqué ci-dessus, le projet de loi a pour première finalité de conférer une base juridique solide à la mise en œuvre de différentes fonctions qui se situent dans le contexte de l'anticipation, de la prévention et de la gestion de crises et qui touchent le domaine de la sécurité numérique, d'une part, et de la communication de crise, d'autre part. Alors que ces fonctions sont déjà exercées aujourd'hui, sous la responsabilité du Haut-Commissariat, par l'ANSSI, le CERT Gouvernemental et le SCC et trouvent leur fondement dans des arrêtés grand-ducaux pris en exécution de l'article 76 de la Constitution,[1] le présent projet de loi vise à conférer, dans un souci de sécurité juridique, une base légale aux fonctions précitées en les intégrant dans la loi portant création d'un Haut-Commissariat à la Protection nationale.

La démarche proposée vise à répondre à une demande du Conseil d'État. En effet, dans son avis complémentaire relatif au projet de loi portant 1. création de l'Autorité nationale de sécurité et 2. modification 1) de la loi du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité ; 2) du Code pénal, la Haute Corporation a retenu que la démarche de conférer des missions à l'ANSSI par le biais d'un arrêté grand-ducal « pouvait encore se concevoir en 2015 du fait que, à ce moment, le Haut-Commissariat à la Protection nationale était constitué en service gouvernemental, tel n'est plus le cas en 2018. La loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale a en effet transformé cette entité gouvernementale en une administration de l'État. Il est dès lors exclu qu'un arrêté trouvant son fondement dans l'article 76 de la Constitution puisse dépasser le cadre de l'organisation du Gouvernement pour conférer de nouvelles attributions, non prévues par la loi, à une administration. Le Conseil d'État invite dès lors le législateur à insérer un article dans la loi en projet à l'effet de modifier la loi précitée du 23 juillet 2016, aux fins d'ajouter aux missions du Haut-Commissariat à la Protection nationale celle d'assurer la fonction de l'ANSSI. »[2] Le Conseil d'État a réitéré son invitation d'ajouter le fonction d'ANSSI aux missions du HCPN dans son avis complémentaire du projet de loi 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'État et 2° la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale.[3]

Afin de donner suite à ces avis du Conseil d'État et de créer in fondement juridique adéquat pour l'exercice de la fonction d'ANSSI, la mission de cette entité gouvernementale est introduite dans la loi-cadre du HCPN. Etant donné que les réflexions développées par le Conseil d'État au sujet de l'ANSSI pourraient également trouver application au niveau du CERT Gouvernemental et du SCC, il est proposé de retenir une démarche similaire pour ces fonctions. Un arrêté grand-ducal abrogera les arrêtés grand-ducaux en question au moment de l'entrée en vigueur de la présente loi.

#### *• L'Agence nationale de la sécurité des systèmes d'information*

En assurant la fonction d'ANSSI, il revient au HCPN de contribuer, à un stade préventif, à la sécurité des réseaux et des systèmes d'information installés et exploités par les administrations et services de l'État en assurant l'élaboration d'une politique générale de sécurité de l'information et de lignes directrices de sécurité de l'information pour des domaines spécifiques.

Une première tentative de légiférer dans le domaine de la sécurité de l'information a été entreprise en 2009 avec le dépôt du projet de loi n° 6075 portant création d'un Centre de Communications du Gouvernement (CCG). Ce texte prévoyait, entre autres, la création de nouvelles missions pour le CCG

---

1 Arrêté grand-ducal du 9 mai 2018 portant fixation de la gouvernance en matière de gestion de la sécurité de l'information, *Mém. A*, n° 423, 29 mai 2018, arrêté grand-ducal du 9 mai 2018 déterminant l'organisation et les attributions du Centre de traitement des urgences informatiques, dénommé « CERT Gouvernemental », *Mém. A*, n° 424, 29 mai 2018 et arrêté grand-ducal du 30 mai 2016 instituant un Service de la communication de crise, *Mém B*, n° 3672, 7 novembre 2019.

2 Doc. parl. n° 6961[3], p. 2.

3 Doc. parl., n° 7314[4], p. 4.

dont « la mise en place d'un service compétent pour les aspects techniques de sécurité des systèmes de communication et d'information appelé Agence nationale de sécurité des systèmes d'information (ANSSI) ».

Or, puisque le projet sous rubrique n'a jamais été soumis au vote de la Chambre des députés et que les visites d'inspection et d'évaluation régulières de l'OTAN ont souligné à plusieurs reprises l'absence d'autorité compétente en matière de sécurité des systèmes d'information, le Gouvernement a décidé en 2015 de mettre en place un cadre pour la gouvernance en matière de gestion de la sécurité de l'information pour l'État par le biais d'un arrêté grand-ducal,[4] en attendant une législation à moyen terme. D'une part, cet arrêté grand-ducal conférait à l'ANSSI des missions dans le domaine de la gouvernance en matière de sécurité de l'information et, d'autre part, la chargeait d'assurer le rôle de gestionnaire des incidents de sécurité affectant les réseaux et les systèmes d'information des administrations et services de l'État.

Au vu des expériences acquises dans le domaine, la structure de la gouvernance en matière de cybersécurité a été adaptée en 2018[5] en établissant une séparation nette entre le volet stratégique et le volet opérationnel de réponse aux incidents et de gestion de crises. Alors que le volet opérationnel est depuis assuré par le CERT Gouvernemental, l'ANSSI agit en amont de tout incident de sécurité en définissant, en concertation avec les entités étatiques concernés, des politiques de sécurité et des lignes directrices couvrant des domaines spécifiques en matière de protection de l'information en vue de permettre aux administrations et services étatiques de prendre les mesures nécessaires pour prévenir la survenance d'incidents de sécurité.

Les recommandations de sécurité émises dans ce cadre sont le résultat d'une approche participative permettant d'associer les acteurs concernés au processus d'élaboration de la politique de sécurité et notamment des politiques couvrant des domaines spécifiques. Cette démarche fut retenue en date du 13 juillet 2018 par le Conseil de Gouvernement sur base des conclusions d'un « proof of concept » que l'ANSSI a réalisé avec le Centre des technologies de l'information de l'État qui est le principal fournisseur d'équipements et de services informatiques auprès de l'État. La politique de sécurité de l'information appliquée auprès de l'État prévoit différents niveaux de sécurité, niveaux qui tiennent compte de la criticité de l'information gérée par une entité, de la taille et de la structure de l'entité, de la complexité technologique des systèmes d'information de l'entité ou encore des besoins et exigences spécifiques de l'entité en matière de sécurité de l'information. Les principaux objectifs recherchés par ce biais consistent à :

– préserver la confidentialité de l'information ;
– assurer l'intégrité de l'information et des processus de gestion de l'information ;
– assurer la disponibilité de l'information ;
– apprécier les risques liés à la sécurité de l'information de façon à adopter des mesures de sécurité appropriées.

Cette mission peut être étendue, à leur demande, aux autres autorités publiques, aux établissements publics, ainsi qu'aux infrastructures critiques.

Alors qu'en 2015, la gouvernance de la sécurité des systèmes d'information classifiés faisait partie des missions de l'ANSSI, cette tâche sera, avec l'entrée en vigueur du projet de loi n° 6961 1. portant création de l'Autorité nationale de sécurité et 2. modification 1) de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité ; 2) du Code pénal assurée par l'Autorité nationale de sécurité (ANS). En effet, la pratique a fait apparaître des questionnements quant aux compétences respectives de l'ANS et de l'ANSSI en matière de protection des informations classifiées. En effet, l'inscription des missions de l'ANSSI en matière de politique de sécurité de l'information classifiée dans la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale aurait pour effet de conférer à deux administrations étatiques – en l'occurrence l'ANS et le HCPN – une compétence partagée mais non clairement délimitée en matière d'élaboration des règles de sécurité de l'information classifiée. Ainsi, dans un souci de consolidation et de cohérence, les missions de l'ANSSI dans le domaine de la régulation de la sécurité des informations classifiées ont été confiées à l'ANS, cela d'autant plus que le domaine de la sécurité des informations classifiées

4 *Mém. A*, n° 30, 20 février 2015, p. 338.
5 *Mém. A*, n° 423, 29 mai 2018.

repose en grande partie sur des exigences qui résultent de directives européennes et de textes de l'OTAN et peuvent ainsi différer des règles de sécurité applicables aux informations non classifiées.

Les missions de l'ANSSI en matière d'élaboration des règles de sécurité sont avant tout d'ordre stratégique et s'inscrivent dans le cadre global de la gouvernance de la sécurité de l'information non-classifiée de l'État. L'ANSSI définit les politiques et les lignes directrices en matière de sécurité de l'information et assiste les services, qui en font la demande, à la mise en place des mesures concernant la sécurité des systèmes d'information. Les missions de l'ANSSI sont complémentaires à la mission d'autres acteurs intervenant au niveau de la sécurité des systèmes d'information opérés par l'État, tels que le CERT Gouvernemental qui assume la gestion opérationnelle des incidents de sécurité d'envergure ou encore les entités qui assurent le fonctionnement opérationnel et partant également la sécurité opérationnelle des systèmes d'information dans les administrations et services de l'État, dont, entre autres, le Centre des technologies de l'information de l'État (CTIE) qui est responsable du déploiement d'une grande partie des systèmes d'information de l'État[6]. A ce titre, le CTIE, de même que tout autre gestionnaire du système informatique d'une administration de l'État – peu importe que cette gestion soit assurée par un service interne ou par un prestataire de service externe – joue un rôle important au niveau de la sécurité informatique dans la mesure que ce gestionnaire doit prendre les mesures opérationnelles nécessaires pour assurer la disponibilité, l'intégrité et la sécurité des systèmes informatiques en place, cela en tenant compte des politiques de sécurité émises par l'ANSSI.

### *• Le CERT Gouvernemental*

Le CERT (*Computer Emergency Response Team*) Gouvernemental est une structure opérationnelle en charge de la gestion des incidents de sécurité affectant, d'une part, les réseaux et systèmes d'information des administrations et services de l'État et, d'autre part, les réseaux et systèmes d'information d'autres autorités publiques, établissements publics et infrastructures critiques si ceux-ci en font la demande.

La gestion des incidents couvre essentiellement la détection des cyberattaques sur les systèmes d'information et la réaction à ces attaques. Elle implique l'animation d'une équipe d'intervention spécialisée capable de prendre en charge la détection et la réponse aux incidents de sécurité d'envergure visant ces réseaux. L'intégration des fonctions en question dans la loi portant création d'un Haut-Commissariat à la Protection nationale permet de créer des synergies évidentes au niveau de la coordination de la mise en œuvre des différentes mesures de prévention et de protection en cas d'attaque d'envergure pouvant conduire à une crise au sens de la loi précitée.

Le CERT Gouvernemental a vu le jour en 2011, dans le cadre de la mise en place de mesures visant à renforcer les moyens de défense du Luxembourg contre les cyberattaques. En effet, le Gouvernement désirait se doter d'une structure opérationnelle apte à réagir à d'éventuelles attaques malveillantes sur les infrastructures informatiques de l'État et procédait ainsi à la création du CERT Gouvernemental.

Depuis, le CERT Gouvernemental a évolué de façon constante. Alors que sa première base réglementaire de 2013[7] lui conférait le pouvoir de prendre en charge la prévention et la gestion des incidents qui menacent ou affectent les systèmes d'information publics et, à leur demande, ceux des infrastructures critiques, le CERT s'est vu attribuer en 2018 les missions de CERT Militaire et de CERT National :

– en tant que CERT Militaire, il revient au CERT Gouvernemental de gérer les incidents de sécurité affectant les réseaux et systèmes d'information de l'Armée luxembourgeoise. Etant donné que le CERT Gouvernemental était de toute façon en charge de la gestion des incidents informatiques d'envergure de la partie du réseau informatique de l'Armée géré par le CTIE et qu'il avait acquis depuis sa création une expertise confirmée en matière de traitement des incidents, il paraissait cohérent de conférer cette nouvelle tâche au CERT Gouvernemental ;

---

6 En effet, le CTIE est certes le plus important fournisseur de la technologie de l'information pour le compte des ministères, administrations et services de l'État. Il est cependant important de souligner que le CTIE n'assure ce service pas pour l'ensemble des administrations et services de l'État qui peuvent soit disposer de leur propre service, soit recourir à un prestataire externe pour couvrir leurs besoins spécifiques en matière de technologies de l'information. A titre d'exemple, citons le Ministère de l'Éducation nationale, de l'Enfance et de la Jeunesse avec le Centre de gestion informatique de l'éducation (CGIE), le Ministère de la Santé, la Police grand-ducale ou encore l'Administration de la navigation aérienne.

7 Arrêté grand-ducal modifié du 30 juillet 2013 déterminant l'organisation et les attributions du Centre gouvernemental de traitement des urgences informatiques, aussi dénommé « Computer Emergency Response Team Gouvernemental », *Mém. A*, n° 161, 6 septembre 2013, p. 3092.

– le CERT National assume le rôle de point de contact national officiel en matière de notification d'incidents de sécurité affectant des réseaux et systèmes d'information sises sur le territoire national. Après réception des notifications, le CERT les relaye au CERT sectoriel compétent. Notons qu'à l'heure actuelle, il y a 10 CERTs enregistrés au Luxembourg.

Il convient de préciser que le CERT Gouvernemental n'intervient jamais directement sur les équipements des entités sous sa compétence. En effet, le rôle du CERT Gouvernemental consiste à assister et à conseiller l'équipe informatique de l'infrastructure concernée sur les actions à prendre.

Remarquons que le CERT Gouvernemental coopère étroitement avec les entités qui assurent le déploiement des systèmes informatiques auprès des administrations et services de l'État comme le CTIE ou le CGIE. En effet, le CERT Gouvernemental possède un mandat qui couvre l'entièreté des réseaux et systèmes d'information de l'État et jouit donc d'une vue globale des incidents qui menacent et impactent les systèmes informatiques étatiques.

***• Le Service de la communication de crise***

A l'instar des développements constatés dans nos pays voisins, le Gouvernement a, en 2016, créé le SCC. D'abord, il revient au SCC de prendre en charge la communication en cas de crise en assurant la coordination horizontale de la communication à l'attention de la population et des médias. Cette entité joue un rôle essentiel au niveau de la gestion d'une crise vu qu'il revient à ce service d'assurer toute communication en situation de crise. Les services de communication des autres entités étatiques qui interviennent au niveau de la gestion d'une crise agissent, le cas échéant, sous la coordination du SCC.

Ensuite, le SCC est chargé d'élaborer une stratégie de communication de crise couvrant aussi bien le volet préventif (actions de sensibilisation et mise au point d'outils de sensibilisation), que la communication en cas de survenance d'une crise.

Afin de pouvoir assurer au mieux ses missions, le SCC collabore étroitement avec les acteurs impliqués dans la prévention et la gestion de crises et établit des relations professionnelles avec les médias luxembourgeois. En outre, le SCC entretient des contacts réguliers avec les services de communication de crise des pays et régions limitrophes.

**2. Adaptation de la définition de l'infrastructure critique**

Le projet de loi limite le champ d'application de la définition de l'infrastructure critique en supprimant le bout de phrase « ou qui est susceptible de faire l'objet d'une menace particulière ». En effet, ces termes font tomber dans la notion d'infrastructure critique des infrastructures qui en temps normaux ne seraient pas considérées critiques, mais qui, au vu de circonstances particulières limitées dans le temps, pourraient faire l'objet d'une menace particulière. Or, puisque les infrastructures critiques sont soumises à des obligations strictes, la désignation d'une infrastructure qui ne serait que momentanément susceptible de faire l'objet d'une menace particulière en tant qu'infrastructure critique, causerait une charge administrative disproportionnée pour cette infrastructure. Au lieu de désigner cette infrastructure en tant qu'infrastructure critique, il est ainsi proposé de recourir dans ces cas aux dispositifs de protection mis en place notamment par la Police grand-ducale et les divers plans d'intervention d'urgence (PIU) du HCPN, tels que le plan gouvernemental de vigilance nationale face aux menaces d'actions terroristes.

**3. Modification de la loi modifiée du 27 février 2011 sur les réseaux et les services de communications électroniques**

Les changements apportés à la loi modifiée du 27 février 2011 sur les réseaux et les services de communications électroniques sont d'ordre purement terminologique. Dans un souci de sécurité juridique et afin de rendre évident que la loi sous rubrique puisse sortir ses effets en cas de crise au sens de la loi-cadre du HCPN, la notion de « crise » au sens de la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale est ajoutée à l'article 5 dont le champ d'application se limite actuellement au conflit armé, la crise internationale grave et la catastrophe.

**4. Modification de la loi modifiée du 8 avril 2018 sur les marchés publics**

Afin de permettre au HCPN de réagir efficacement en cas de prévention et de gestion de crises, le livre I$^{er}$ de la loi sur les marchés publics est adapté à deux égards.

D'abord, il est permis au HCPN de recourir, sous certaines conditions, à une procédure restreinte sans publication d'avis ou à une procédure négociée pour la passation de marchés de travaux. En effet, depuis 2016, le Haut-Commissariat à la Protection nationale était confronté, à plusieurs reprises, à des intempéries qualifiées de « crise » au sens de la loi HCPN et ayant causé des dommages importants aux biens étatiques et communaux. Bien que la remise en état des infrastructures essentielles bénéficiait dans une première phase des dispositions d'urgence de la loi sur les marchés publics (art. 20, paragraphe 1er, lettre f)), la complexité de certains dossiers a eu pour effet de prolonger les travaux de réparation dans le temps, de sorte que les travaux étaient encore en cours de réalisation alors que la première phase d'urgence venait à son terme. En effet, il se peut, vu la complexité des travaux à réaliser, que des études statiques approfondies doivent être réalisées au préalable pour examiner l'étendue précise des dégâts. L'absence de la notion de « travaux » dans l'article 20, paragraphe 1er, lettre m), de la loi modifiée du 8 avril 2018 sur les marchés publics, a rendu inutilement compliquée la remise en état de ces infrastructures. Il est entendu que la formulation proposée ne permet le recours à la procédure négociée qu'au cas où la réparation en tant que telle s'avère urgente. Remarquons que le HCPN bénéficie déjà à l'heure actuelle de cette prérogative pour la passation de marchés de fournitures et de services.

Ensuite, le projet de loi exempte le HCPN de l'obligation de devoir solliciter l'avis préalable de la Commission des soumissions en cas d'urgence impérieuse. En effet, les situations d'urgence impérieuse sont par la force des choses, et par définition, incompatibles avec l'accomplissement d'une formalité de demande d'avis préalable. En témoignent les marchés qui ont dû être passés au pied levé dans le contexte de la lutte contre la propagation du COVID-19, où le HCPN essayait d'acquérir des équipements de protection individuelle essentiels, sur un marché dans lequel la demande dépassait de loin l'offre et dans un contexte international difficile, tel que documenté par la presse internationale. Il s'agissait de répondre instantanément aux offres reçues, le cas échéant, sous peine de voir un autre acquéreur s'emparer des fournitures.

### 5. Adaptations en matière de personnel

Finalement, le nouveau projet de loi entérine formellement la fonction de Haut-Commissaire à la Protection nationale adjoint. Alors que cette fonction existe dans l'organigramme du HCPN depuis 2016, il revient au projet de loi de lui accorder une base légale. Puisque le HCPN ne cesse de gagner en missions depuis 2015, notamment au vu des missions d'ANSSI, de CERT Gouvernemental et de SCC, il est opportun de créer la fonction de Haut-Commissaire adjoint. Il y a lieu de noter en outre qu'une des deux personnes qui assurent la direction du HCPN doit se trouver en permanence sur le territoire national pour être en mesure d'intervenir en cas de crise.

Ensuite, à l'instar des dispositions prévues pour le personnel du cadre civil de la Police grand-ducale et de l'Inspection générale de la Police, la nouvelle loi prévoit une prime d'astreinte de 12 points indiciaires pour le personnel du HCPN soumis à une obligation de permanence ou de présence.

*

## COMMENTAIRE DES ARTICLES

*Ad article Ier*

L'article Ier, point 1, modifie l'article 2, point 4, de la loi modifiée portant création d'un Haut-Commissariat à la Protection nationale (HCPN) en supprimant de la définition de « l'infrastructure critique » les termes « ou qui est susceptible de faire l'objet d'une menace particulière ». Il s'est avéré que ces termes dépassent ce qui est réellement visé par la notion d'infrastructure critique. En effet, interprété à la lettre, ces termes font tomber dans la notion d'infrastructure critique des infrastructures qui en temps normaux ne seraient pas considérées critiques, mais qui, au vu de circonstances particulières limitées dans le temps, pourraient faire l'objet d'une menace particulière. Or, puisque les infrastructures critiques sont soumises à des obligations strictes, la désignation d'une infrastructure qui ne serait que momentanément susceptible de faire l'objet d'une menace particulière en tant qu'infrastructure critique, causerait une charge administrative disproportionnée pour cette infrastructure. Au lieu de désigner cette infrastructure en tant qu'infrastructure critique, il est ainsi proposé de recourir dans ces cas aux dispositifs de protection mis en place notamment par la Police grand-ducale et les

divers plans d'intervention d'urgence (PIU) du HCPN, tels que le plan gouvernemental de vigilance nationale face aux menaces d'actions terroristes.

Remarquons que cette interprétation est en ligne avec les deux règlements grand-ducaux pris en matière d'infrastructures critiques.[8]

L'article I[er], point 2, rajoute la définition de la « sécurité de l'information » dans la loi-cadre du HCPN. Etant donné que la fonction d'Agence nationale de la sécurité des systèmes d'information (ANSSI) est inscrite dans la loi portant création d'un Haut-Commissariat à la Protection nationale et que cette fonction concerne notamment la sécurité de l'information, il a été jugé nécessaire de reprendre au niveau de la loi-cadre du HCPN la définition de la notion qui figure dans l'arrêté grand-ducal du 9 mai 2018 portant fixation de la gouvernance en matière de gestion de la sécurité de l'information. Puisque le projet de loi n° 6961 1. portant création de l'Autorité nationale de sécurité et 2. modification 1) de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité ; 2) du Code pénal confie les missions de l'ANSSI en matière de régulation de la sécurité des informations classifiées à l'Autorité nationale de sécurité (ANS), la définition de la « sécurité de l'information » est adaptée. Il est ainsi souligné que les compétences du HCPN ne concernent que la sécurité des réseaux et systèmes d'information non classifiés et visent, conformément à la stratégie élaborée dans ce domaine au cours des dernières années, a priori, les administrations et services de l'État.

L'article I[er], point 3, du projet de loi vise, dans un souci de sécurité juridique, à accorder une base légale aux fonctions d'ANSSI, de Centre de traitement des urgences informatiques (CERT Gouvernemental) et de Service de la communication de crise (SCC), réglementés à date par le biais de trois arrêtés grand-ducaux. Les missions des différents services sont précisées *infra*.

L'article I[er], point 4, rajoute trois nouveaux chapitres dans la loi-cadre du HCPN. D'abord, l'article I[er], point 3 attribue au HCPN la fonction d'ANSSI, de sorte que les missions afférentes dans le domaine de la sécurité de l'information seront inscrites dans la loi-cadre du HCPN.

En assurant la fonction d'ANSSI, le HCPN définit la politique générale de sécurité de l'information de l'État à l'adresse des administrations et services de l'État (paragraphe 1[er], lettre a)). Alors que la notion de « politique de sécurité de l'information » trouve son origine dans la norme ISO/CEI 27000 qui pose les exigences de sécurité à appliquer dans le secteur privé, l'ANSSI a, en étroite collaboration avec les acteurs-clé du domaine de la sécurité informatique de l'État, tels que le Centre des technologies et de l'information de l'État (CTIE) et le CERT Gouvernemental, élaboré une politique de sécurité adaptée au contexte étatique.

Cette politique, dont une deuxième édition a vu le jour en 2018, a pour objet de définir des mesures de sécurité dans le domaine de la protection de l'information gérée par les administrations et services de l'État, afin d'en garantir la confidentialité, l'intégrité et la disponibilité. La politique générale de sécurité de l'information de l'État décrit les objectifs généraux de sécurité de l'information, ses principes fondateurs et le cadre organisationnel de la gestion de la sécurité de l'information de l'État. Soulignons que la politique de sécurité de l'ANSSI n'a pas de force contraignante et que la responsabilité de mettre en place les mesures techniques et organisationnelles nécessaires pour garantir la sécurité de l'information appartient aux administrations et services étatiques.

Remarquons que le volet de la sécurité des systèmes d'information classifiés ne fait plus partie des compétences de l'ANSSI. En effet, dans un souci de cohérence, il a été décidé de confier cette mission à l'ANS qui, selon le projet de loi n° 6961 1. portant création de l'Autorité nationale de sécurité et 2. modification 1) de la loi modifiée du 15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité ; 2) du Code pénal est « responsable de la définition des dispositions de sécurité destinées à assurer la protection des pièces classifiées. » Ainsi, l'ANSSI assurera dorénavant le volet de la sécurité de l'information non-classifiée, tandis que l'ANS est compétente pour le volet de la sécurité des informations classifiées.

Outre la politique générale, l'ANSSI est compétente pour définir, en concertation avec les administrations et services de l'État concernés, des politiques et lignes directrices de sécurité pour des domaines spécifiques et d'émettre des recommandations d'implémentation y relatives (lettre b)). Ces politiques

---

8 Règlement grand-ducal du 21 février 2018 fixant la structure des plans de sécurité et de continuité de l'activité des infrastructures critiques, *Mém. A*, n° 151, 1[er] mars 2018 et règlement grand-ducal du 21 février 2018 déterminant les modalités du recensement et de la désignation des infrastructures critiques, *Mém. A*, n° 152, 1[er] mars 2018.

sont spécifiques dans le sens où elles ne concernent qu'un certain domaine de la sécurité de l'information, tel que la sécurité physique et environnementale, le contrôle d'accès, la sécurité des communications ou encore la sécurité des ressources humaines. Alors que l'ANSSI élaborerait une politique dans le domaine de la sécurité des ressources humaines ensemble avec le Centre de gestion du personnel et de l'organisation de l'État (CGPO), une politique en matière de sécurité physique et environnementale serait formulée en coopération avec l'Administration des bâtiments publics (ABP).

Après avoir défini les politiques et lignes directrices, l'ANSSI assiste les entités qui en font la demande dans l'implémentation de ces politiques de sécurité. Vu les spécificités de chaque entité, il importe d'identifier les objectifs de sécurité qui leurs sont propres avant de définir les mesures de sécurité appropriées.

Selon la lettre c), la troisième mission de l'ANSSI tourne autour de la gestion des risques en matière de sécurité de l'information. La gestion des risques s'appuie sur un processus systématique d'identification, d'appréciation et de traitement des risques et permet d'assurer que les mesures de protection mises en place sont proportionnées aux enjeux et aux risques encourus.

L'ANSSI a mis en œuvre une méthodologie d'analyse des risques pragmatique, facile à appréhender et adaptée à la structure et au fonctionnement des différents types d'entités étatiques. Depuis fin 2018, elle propose aux entités intéressées, sans frais à leurs charges, un accompagnement professionnel à la réalisation d'une première analyse des risques et à la définition d'un plan de traitement des risques. Cette analyse des risques permet de sélectionner et prioriser les mesures appropriées à mettre en œuvre au niveau de la sécurité de l'information.

Conformément à la lettre d), l'ANSSI conseille l'INAP et les entités qui en font la demande dans la définition de programmes de formation relatifs à la sécurité de l'information. Tandis que les formations générales en matière de sécurité de l'information s'adressent à tout le personnel de l'État, les programmes de formation couvrant des domaines plus spécifiques de la sécurité de l'information s'adressent aux responsables de la gestion de la sécurité de l'information et aux professionnels des technologies de l'information et de communication.

En sus, l'ANSSI a la mission de promouvoir la sécurité de l'information (lettre e)). En effet, la sécurité de l'information repose avant tout sur des mesures simples et des bonnes pratiques à adopter par toutes les parties prenantes. La sensibilisation aux risques cyber et aux mesures de prévention et de protection constitue le premier moyen de défense pour garantir la sécurité des réseaux et des systèmes d'information. De cette manière, l'ANSSI entend instaurer une véritable culture de la sécurité de l'information au sein de l'ensemble du personnel de l'État.

Finalement, l'ANSSI assure la fonction d'autorité TEMPEST (lettre f)). Puisque tout équipement ou système qui traite ou transmet des informations sous forme électronique produit des signaux électromagnétiques et que ces signaux peuvent être représentatifs des informations traitées, leur interception et leur exploitation risquent de révéler des informations sensibles à des destinataires malveillants. Une telle interception et exploitation de signaux en vue d'une reconstitution d'informations traitées constitue la « menace TEMPEST ».

Le risque lié à l'interception et à l'exploitation de signaux compromettants est particulièrement présent dans le domaine des informations classifiées. Ainsi, afin d'assurer la protection des informations classifiées traitées par les réseaux et systèmes d'information, l'OTAN et l'UE imposent que chaque État membre mette en place une autorité TEMPEST qui est chargée :

– de veiller à la conformité des réseaux et systèmes d'information classifiés aux stratégies et lignes directrices TEMPEST, et
– d'approuver les contre-mesures TEMPEST pour les installations et les produits destinés à protéger des informations classifiées. Les contre-mesures sont déterminées en fonction du niveau de classification des informations traitées, de l'affaiblissement électromagnétique naturel du bâtiment/local (« zonage TEMPEST »), de la proximité éventuelle d'éléments extérieurs non contrôlés et des caractéristiques de rayonnement électromagnétique des équipements. Les mesures de protection ainsi identifiées s'étendent de la simple mise en place de matériel de traitement certifiée à un certain niveau de protection TEMPEST (matériel TEMPEST certifié niveau A, B ou C selon la norme SDIP 27/2 de l'OTAN) à la mise en place d'une cage Faraday, enceinte blindée empêchant la propagation d'ondes électromagnétiques.

Le paragraphe 2 pose que les activités de l'ANSSI peuvent être étendues, à leur demande, à d'autres autorités publiques, aux établissements publics et infrastructures critiques. Les « autres autorités

publiques » visent les entités qui ne seraient pas des administrations et services étatiques, tels que la Chambre des députés. L'extension aux infrastructures critiques est une conséquence logique de l'intégration des fonctions de l'ANSSI dans la loi-cadre du HCPN qui est l'autorité compétente en matière de protection des infrastructures critiques. De cette façon, afin de pouvoir garantir un suivi optimal de ces infrastructures, le HCPN aura la possibilité de leur proposer les services de l'ANSSI pour ce qui est du volet de leur sécurité de l'information.

Cette extension des fonctions d'ANSSI aux infrastructures critiques ne peut se faire, conformément à la philosophie inhérente à la loi portant création d'un HCPN, qu'à la demande du propriétaire ou de l'opérateur d'une infrastructure critique. En effet, le législateur, en formulant les dispositions régissant la protection des infrastructures critiques qui sont inscrites dans la loi portant création d'un HCPN, a privilégié une approche de collaboration entre le HCPN et les opérateurs d'une infrastructure critique, cela par opposition à une approche dirigiste consistant à imposer à ces opérateurs des mesures contraignantes. Ainsi, le HCPN, après avoir analysé le plan de continuité de l'activité d'une infrastructure critique, peut formuler des recommandations au niveau des mesures de sécurité à implémenter auprès d'une infrastructure critique en vue d'en renforcer la résilience. Dans le contexte de cette analyse, le HCPN peut évidemment émettre des recommandations concernant la sécurité de l'information et proposer à ce niveau ses services de conseil.

Ensuite, l'article I$^{er}$, point 4, rajoute un nouvel chapitre 4*quater* dans la loi-cadre du HCPN qui attribue la mission de CERT (*Computer Emergency Response Team*) Gouvernemental au HCPN (article 9*quater*). Les missions du CERT Gouvernemental sont complémentaires à celles de l'ANSSI. En effet, alors que les attributions de l'ANSSI se situent dans le domaine de la prévention, celles du CERT Gouvernemental s'inscrivent dans le domaine de la réaction. Le CERT Gouvernemental est une structure opérationnelle ayant comme mission principale de détecter les attaques informatiques dirigées à l'encontre des réseaux informatiques de l'État et d'organiser une réaction adéquate à ces attaques.

La compétence du CERT Gouvernemental vise les « incidents de sécurité d'envergure », c'est-à-dire les incidents qui impactent la disponibilité, l'intégrité ou la confidentialité des systèmes d'information de l'État. Ces incidents d'envergure sur les réseaux et systèmes sont à distinguer des évènements de sécurité, qui constituent de simples risques de compromission des équipements ou logiciels déployés auprès de l'État.

La lettre a) du paragraphe 1$^{er}$ attribue au CERT Gouvernemental une compétence transversale en matière de gestion des incidents de sécurité d'envergure en le nommant « point de contact unique ». En effet, un centre de traitement centralisé permet de mettre sur pied une équipe d'experts capable de prendre en charge de manière rapide des attaques sophistiquées.

Selon la lettre b), la réponse du CERT Gouvernemental aux incidents informatiques se divise en plusieurs étapes :

D'abord, le CERT Gouvernemental organise une veille technologique portant sur les différents types d'attaques, ainsi que sur les moyens de défense y relatifs. Les informations sont rassemblées à l'aide de sources ouvertes, telles que des sites d'actualités spécialisés, de sources commerciales et d'échanges avec des partenaires.

Ensuite, il revient au CERT Gouvernemental de détecter les incidents de sécurité d'envergure affectant les réseaux et systèmes d'information de l'État à travers des analyses manuelles ou automatiques (par exemple logiciels du type *endpoint protection* qui permettent de sécuriser à distance les terminaux des utilisateurs). Plus précisément, l'équipe du CERT Gouvernemental examine les fichiers de journalisation (*logs*) générés par les équipements informatiques afin d'identifier une compromission éventuelle (*indicators of compromise*). Notons que le CERT Gouvernemental reçoit constamment des indicateurs de compromission de ses partenaires nationaux et internationaux, de sorte qu'il lui est possible de mettre en place des logiciels qui trouvent ces indicateurs.

Lors de la phase d'alerte, le CERT Gouvernemental met en garde le correspondant informatique de l'entité compromise pour que ce dernier puisse prendre les mesures de réaction appropriées.

Dernièrement, pendant la phase de réaction, le CERT Gouvernemental propose des mesures de remédiation, soit au correspondant informatique, soit à l'opérateur de systèmes (par exemple le CTIE). En effet, il convient de noter que le CERT Gouvernemental a une fonction de conseil et de support pour les entités concernées, sans pour autant intervenir directement sur l'équipement électronique de ces derniers.

La lettre c) du premier paragraphe décrit la fonction de centre national de traitement des urgences informatiques, dénommé CERT National. Afin d'éviter toute confusion au niveau du CERT compétent

pour un incident donné, le CERT National agit en tant que point de contact national compétent pour recevoir toute notification d'incidents et pour relayer ces informations au CERT sectoriel compétent. Observons que la mission du CERT National s'arrête à la transmission de l'incident au CERT compétent et que le CERT National n'assure par conséquent aucun suivi des incidents transmis. Les informations qui sont reçues par le CERT Gouvernemental dans le cadre de sa mission de CERT National de la part de ses partenaires internationaux et des opérateurs d'infrastructures critiques lui permettent d'avoir une vue d'ensemble pour évaluer correctement l'état de la sécurité dans le domaine cyber et pour anticiper ainsi les mesures qui s'imposent. Il opère comme point de contact officiel pour les CERTs national étrangers et pour la collecte et la distribution d'informations relatives aux incidents de sécurité concernant les systèmes d'information localisés au Luxembourg et de relayer les informations pertinentes aux CERTs sectoriels.

Finalement, le HCPN est en charge de la fonction de CERT Militaire (lettre d)). En tant que CERT Militaire, il lui revient d'assurer la gestion des incidents informatiques survenant sur les réseaux et systèmes d'information de l'Armée luxembourgeoise. En effet, l'Armée luxembourgeoise a fait connaître son besoin de faire protéger ses infrastructures informatiques opérationnelles. Il est entendu que les interventions du CERT Gouvernemental se limiteront à des interventions pouvant être réalisées à partir du territoire national et que le personnel du HCPN ne peut être appelé à se déplacer à l'étranger pour réaliser ces interventions.

A l'instar du domaine de compétence de l'ANSSI, le deuxième paragraphe de l'article 9*quater* permet au CERT Gouvernemental de proposer ses services à d'autres autorités publiques, aux établissements publics, ainsi qu'aux infrastructures critiques. Ces services sont fournis sur base d'un accord de collaboration qui définit les responsabilités de chaque partie. Ces accords permettent au CERT Gouvernemental d'obtenir des informations sur les attaques dirigées à l'encontre de ces entités et d'utiliser ces informations pour protéger le reste de sa constituante. Ce cas de figure rejoint la mission de CERT National, en l'occurrence une mission d'intérêt général, à savoir la protection des besoins essentiels et des intérêts vitaux de la population et du pays. Conformément à la philosophie de la loi portant création d'un HCPN, l'opérateur d'une infrastructure critique reste libre de recourir aux services du CERT Gouvernemental. Ainsi, par exemple, dans le contexte de l'analyse du plan de continuité des activités d'une infrastructure critique, le HCPN peut recommander à ce que l'opérateur de l'infrastructure critique collabore avec un CERT. L'opérateur est cependant libre de recourir aux services du CERT Gouvernemental ou aux services d'un des dix CERTs exerçant des activités au Luxembourg.

A l'heure actuelle, des de collaboration ont été conclus avec des entités nationales, telles que la Banque et la Caisse d'Epargne de l'État et le Corps grand-ducal d'incendie et de secours, et internationales sises sur le territoire luxembourgeois, telles que la *NATO Support and Procurement Agency*.

Le troisième paragraphe pose que le CERT Gouvernemental bénéficie de la part des administrations et services de l'État de toute collaboration nécessaire. Cette collaboration implique notamment que le CERT Gouvernemental est autorisé à recueillir, demander et obtenir des informations à caractère technique sur les infrastructures et architectures de communication et d'information et de recueillir, demander et obtenir un accès aux fichiers de journalisation techniques. En outre, le CERT Gouvernemental peut demander aux administrations et services de l'État de déconnecter des équipements informatiques des réseaux de communication de l'État.

Outre l'ANSSI et le CERT Gouvernemental, le SCC sera intégré dans la loi portant création d'un Haut-Commissariat à la Protection nationale (nouvel chapitre 4*quinquies* (article 9*quinquies*) de la loi-cadre du HCPN). Le SCC est appelé à élaborer une stratégie de communication de crise couvrant aussi bien le volet préventif (actions de sensibilisation et mise au point d'outils de sensibilisation), que la communication en cas de survenance d'une crise. Dans ce contexte, il lui revient, d'une part, d'émettre des consignes et alertes à destination de la population afin de réduire les impacts de la crise et, d'autre part, de limiter les polémiques qui risquent de se propager à défaut de communication adéquate.

Afin de pouvoir assurer au mieux ses missions, le SCC collabore étroitement avec les acteurs impliqués dans la prévention et la gestion de crises et établit des relations professionnelles avec les médias luxembourgeois. En outre, le SCC entretient des contacts réguliers avec les services de communication de crise des pays et régions limitrophes.

L'article I$^{er}$, point 5, de la loi sous projet consacre formellement la fonction de Haut-Commissaire à la Protection nationale adjoint qui existe depuis 2016 dans l'organigramme du HCPN. Puisque le

HCPN s'est vu attribuer au cours des dernières années de plus en plus de missions, un renfort au niveau de la direction s'avère indispensable.

L'article I^er^, point 6, complète le cadre du personnel par la fonction du Haut-Commissaire à la Protection nationale adjoint (article 11, paragraphe 1^er^) et supprime l'article 11, paragraphe 2, alinéa 2 de la loi portant création d'un Haut-Commissariat à la Protection nationale. En effet, afin de diminuer la charge administrative en relation avec le détachement d'un agent auprès du HCPN, il est décidé de se rallier au régime de droit commun fixé par l'article 7, paragraphe 2, de la loi modifiée du 16 avril 1979 fixant le statut général des fonctionnaires de l'État.

L'article I^er^, point 7, contient les dispositions nécessaires pour assurer le transfert du personnel de l'ANSSI, du CERT Gouvernemental et du SCC vers le Haut-Commissariat à la Protection nationale. En effet, il y a lieu de prévoir des garde-fous pour éviter que les agents disposant d'une majoration d'échelon ou d'un grade de substitution ne soient lésés par ce transfert. Il s'agit de souligner qu'il s'agit d'une mesure transitoire dont l'effet disparaîtra au plus tard avec la cessation des fonctions des agents concernés.

*Ad article II*

Etant donné que la fonction de Haut-Commissaire à la Protection nationale adjoint est introduite dans la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale (HCPN) et que cette fonction est à considérer comme fonction dirigeante, il importe de l'insérer dans la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'État.

*Ad article III*

La terminologie utilisée au niveau de l'article 5 de loi modifiée du 27 février 2011 sur les réseaux et les services de communications électroniques est alignée sur celle qui a été inscrite dans la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, cette dernière ayant introduit dans notre ordre juridique une définition de la notion de « crise ». L'adaptation vise ainsi à assurer que le dispositif inscrit à l'article 5 précité puisse être mis en œuvre en cas de crise, et notamment dans le contexte d'une crise se situant dans le cadre du « Plan d'intervention d'urgence face aux attaques contre les systèmes d'information ou en cas de défaillance des systèmes d'information ».

*Ad article IV*

L'article du projet de loi modifie la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État sur deux points.

D'abord, la fonction du Haut-Commissaire à la Protection nationale adjoint est insérée à l'article 17, de sorte que cette fonction va de pair avec une majoration d'échelon pour fonctions dirigeantes.

En outre, l'article 22 de ladite loi est complété par un nouvel paragraphe qui accorde une prime de 12 points indiciaires aux agents du HCPN qui sont soumis à une obligation de permanence ou de présence. En effet, vu que le HCPN est un organe de gestion de crise qui doit pouvoir être joignable en permanence, certains agents sont soumis à une obligation de permanence. Cet ajout vise à compenser les efforts mis en œuvre par ces agents.

Finalement, à l'instar des dispositions applicables aux directeurs adjoints d'autres administrations, le point 4 de l'article IV prévoit des allongements de grade pour la fonction du Haut-Commissaire à la Protection nationale adjoint.

*Ad article V*

Le projet sous rubrique modifie la loi modifiée du 8 avril 2018 sur les marchés publics est modifiée à deux égards.

D'abord, comme la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale assure un accès rapide aux fournitures et services en cas de crise, l'article V vise à inclure les marchés de travaux dans le champ d'application de ce régime d'exception. En effet, depuis 2016, le Haut-Commissariat à la Protection nationale était confronté, à plusieurs reprises, à des intempéries qualifiées de « crise » au sens de la loi HCPN et ayant causé des dommages importants aux biens étatiques et communaux. Bien que la remise en état des infrastructures essentielles bénéficiait

dans une première phase des dispositions d'urgence de la loi sur les marchés publics (art. 20, paragraphe 1er, lettre f)), la complexité de certains dossiers a eu pour effet de prolonger les travaux de réparation dans le temps, de sorte que les travaux étaient encore en cours de réalisation alors que la première phase d'urgence venait à son terme. En effet, il se peut, vu la complexité des travaux à réaliser, que des études statiques approfondies doivent être réalisées au préalable pour examiner l'étendue précise des dégâts. L'absence de la notion de « travaux » dans l'article 20, paragraphe 1er, lettre m), de la loi modifiée du 8 avril 2018 sur les marchés publics, a rendu inutilement compliquée la remise en état de ces infrastructures. Il est entendu que la formulation proposée ne permet le recours à la procédure négociée qu'au cas où la réparation en tant que telle s'avère urgente.

Soulignons que ce régime d'exception est limité aux marchés tombant dans le champ d'application du livre Ier de la loi sur les marchés publics, de sorte que les marchés publics de travaux d'envergure (au-dessus de 5.186.000 EUR) sont passés avec les mesures de publicité adéquates.

Ensuite, afin de permettre au HCPN de répondre de manière efficace à une crise, le projet de loi modifie l'article 159, paragraphe 3, de la loi modifiée du 8 avril 2018 sur les marchés publics. En effet, alors que les articles 20, paragraphe 1er, lettre f), 64, paragraphe 2, lettre c), et 124, lettre d) de la loi modifiée du 8 avril 2018 sur les marchés publics permettent au HCPN de recourir à une procédure restreinte sans publication d'avis ou une procédure négociée dès lors que les conditions de « l'urgence impérieuse », telles qu'énoncées dans le cadre de ces dispositions, sont remplies (ce qui est bien souvent le cas en temps de crise), la passation de ces marchés est retardée par le fait qu'un avis doit préalablement être sollicité auprès de la Commission des soumissions. Or, les situations d'urgence impérieuse sont par la force des choses, et par définition, incompatibles avec l'accomplissement d'une formalité de demande d'avis préalable. En témoignent les marchés qui ont dû être passés au pied levé dans le contexte de la lutte contre la propagation du COVID-19, où le HCPN essayait d'acquérir des équipements de protection individuelle essentiels, sur un marché dans lequel la demande dépassait de loin l'offre et dans un contexte international difficile, tel que documenté par la presse internationale. Il s'agissait de répondre instantanément aux offres reçues, le cas échéant, sous peine de voir un autre acquéreur s'emparer des fournitures. Le projet de loi est formulé de manière à ce que l'exemption à l'obligation de saisir préalablement la Commission des soumissions, telle que prévue à l'article 159, paragraphe 3, soit strictement limitée.

*

# TEXTES COORDONNES

## LOI MODIFIEE DU 23 JUILLET 2016

**portant création d'un Haut-Commissariat à la Protection nationale et modifiant**

**a) la loi modifiée du 23 juillet 1952 concernant l'organisation militaire ;**

**b) la loi du 8 décembre 1981 sur les réquisitions en cas de conflit armé, de crise internationale grave ou de catastrophe ;**

**c) la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel ;**

**d) la loi modifiée du 25 juin 2009 sur les marchés publics ;**

**e) la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'Etat ;**

**f) la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat**

### Chapitre 1er – Objet

**Art. 1er.** Il est créé une administration dénommée Haut-Commissariat à la Protection nationale, dont les compétences et les mécanismes selon lesquels elle intervient sont déterminés par la présente loi qui règle également l'organisation de la protection des infrastructures critiques.

Le Haut-Commissariat à la Protection nationale est placé sous l'autorité du membre du Gouvernement ayant dans ses attributions la Protection nationale.

### Chapitre 2 – Définitions

**Art. 2.** Pour l'application de la présente loi, on entend par

1. « concept de protection nationale » : un concept qui consiste à prévenir les crises, respectivement à protéger le pays et la population contre les effets d'une crise. En cas de survenance d'une crise, il comprend la gestion des mesures et activités destinées à faire face à la crise et à ses effets et à favoriser le retour à l'état normal ;
2. « crise » : tout évènement qui, par sa nature ou ses effets, porte préjudice aux intérêts vitaux ou aux besoins essentiels de tout ou partie du pays ou de la population, qui requiert des décisions urgentes et qui exige une coordination au niveau national des actions du Gouvernement, des administrations, des services et organismes relevant des pouvoirs publics, et, si besoin en est, également au niveau international ;
3. « gestion de crises » : l'ensemble des mesures et activités que le Gouvernement initie, le cas échéant avec le concours des autorités communales concernées, pour faire face à la crise et à ses effets et pour favoriser le retour à l'état normal ;
4. « infrastructure critique » : tout 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~~ ;

4*bis*. « sécurité de l'information » : sécurité autour des réseaux et systèmes d'information non classifiés installés et exploités par les administrations et services de l'État ;

5. « stratégie nationale en matière de sécurité des réseaux et des systèmes d'information » : un cadre prévoyant des objectifs et priorités stratégiques en matière de sécurité des réseaux et des systèmes d'information au niveau national.

## Chapitre 3 – Mission et attributions du Haut-Commissariat à la Protection nationale

**Art. 3.** (1) Le Haut-Commissariat à la Protection nationale a pour mission de mettre en œuvre le concept de protection nationale tel que défini à l'article 2. Dans le cadre de cette mission, le Haut-Commissariat à la Protection nationale a pour attributions

a) quant aux mesures de prévention de crises :

1. de coordonner les contributions des ministères, administrations et services de l'État ;
2. de coordonner les politiques, les projets et les programmes de recherche ;
3. de procéder à l'analyse des risques et à l'organisation d'une veille ;
4. de coordonner l'organisation des cours de formation et des exercices ;

b) quant aux mesures d'anticipation de crises :

1. de développer et de coordonner une stratégie nationale de gestion de crises ;
2. de définir la typologie, la structure, le corps et le format des plans déclinant les mesures et activités de prévention et de gestion de crises et de coordonner la planification ;
3. d'initier, de coordonner et de veiller à l'exécution des activités et mesures relatives au recensement, à la désignation et à la protection des infrastructures critiques, qu'elles soient publiques ou privées ;
4. de coordonner et d'élaborer une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information ;

c) quant aux mesures de gestion de crises :

1. d'initier, de conduire et de coordonner les tâches de gestion de crises ;
2. de veiller à l'exécution de toutes les décisions prises ;
3. de favoriser le plus rapidement possible le retour à l'état normal ;
4. de préparer un budget commun pour la gestion de crises et de veiller à son exécution ;
5. de veiller à la mise en place et au fonctionnement du Centre national de crise.

Dans le cadre de ses attributions, le Haut-Commissariat à la Protection nationale est le point de contact du Luxembourg auprès des institutions et organisations européennes et internationales et veille à une coopération efficace avec ces entités.

(1*bis*) Le Haut-Commissariat à la Protection nationale assure les fonctions d'Agence nationale de la sécurité des systèmes d'information, ci-après « ANSSI », de Centre de traitement des urgences informatiques, ci-après « CERT Gouvernemental » et de Service de la communication de crise.

(2) Les autorités administratives et judiciaires, la Police grand-ducale et le Haut-Commissariat à la Protection nationale veillent à assurer une coopération efficace en matière de communication des informations susceptibles d'avoir un rapport avec leurs missions.

(3) Le Haut-Commissaire à la Protection nationale ou son délégué peuvent, par demande écrite, demander à tout détenteur d'un secret professionnel ou d'un secret protégé par une clause contractuelle la communication des informations couvertes par ce secret si la révélation dudit secret est nécessaire à l'exercice de sa mission de gestion de crises ou de protection des infrastructures critiques. Une divulgation d'informations en réponse à une telle demande n'entraîne pour l'organisme ou la personne détenteur des informations secrètes aucune responsabilité.

(4) Les informations qui sont couvertes par le secret de l'instruction relative à une enquête judiciaire concomitante ne peuvent être transmises qu'avec l'accord de la juridiction ou du magistrat saisi du dossier.

## Chapitre 4 – La protection des infrastructures critiques

**Art. 4.** La protection de l'infrastructure critique comprend l'ensemble des activités visant à prévenir, à atténuer ou à neutraliser le risque d'une réduction ou d'une discontinuité de la disponibilité de four-

nitures ou de services indispensables à la sauvegarde des intérêts vitaux ou des besoins essentiels de tout ou partie du pays ou de la population offerts par l'intermédiaire de l'infrastructure ainsi que le risque externe dont l'infrastructure est susceptible de faire l'objet.

Un point, système ou partie de celui-ci ne répondant pas à la définition donnée à l'article 2, peut être recensé et classifié comme infrastructure critique lorsque le fonctionnement d'une infrastructure critique en dépend.

De même peut être recensé et désigné comme infrastructure critique un secteur ou une partie de secteur dont tous les éléments ne répondent pas nécessairement à la définition donnée à l'article 2, mais dont l'ensemble est considéré comme tel.

**Art. 5.** Les modalités du recensement et de la désignation des infrastructures critiques sont fixées par règlement grand-ducal.

**Art. 6.** Le propriétaire ou opérateur d'une infrastructure critique est tenu de mettre à la disposition du Haut-Commissariat à la Protection nationale toutes les données sollicitées aux fins du recensement, de la désignation et de la protection des infrastructures critiques. Ces données comprennent toutes les informations qui sont nécessaires dans le contexte de la prévention ou de la gestion d'une crise.

Les données relatives à l'infrastructure critique faisant l'objet d'un enregistrement, d'une communication, d'une déclaration, d'un recensement, d'un classement, d'une autorisation ou d'une notification imposés par la loi ou par la réglementation afférente sont communiquées au Haut-Commissariat à la Protection nationale, sur sa demande, par les départements ministériels, les administrations et services de l'État qui détiennent ces données.

**Art. 7.** La désignation d'une infrastructure critique fait l'objet d'un arrêté grand-ducal.

**Art. 8.** (1) Le propriétaire ou opérateur d'une infrastructure critique est tenu d'élaborer un plan de sécurité et de continuité de l'activité qui comporte les mesures de sécurité pour la protection de l'infrastructure. Le Haut-Commissariat à la Protection nationale adresse au propriétaire ou à l'opérateur d'une infrastructure critique des recommandations concernant ces mesures de sécurité qui permettent d'en assurer la protection au sens de l'article 4, d'en améliorer la résilience et de faciliter la gestion d'une crise.

(2) Le propriétaire ou opérateur d'une infrastructure critique est tenu de désigner un correspondant pour la sécurité qui exerce la fonction de contact pour les questions liées à la sécurité de l'infrastructure avec le Haut-Commissariat à la Protection nationale.

(3) Le propriétaire ou opérateur d'une infrastructure critique doit notifier au Haut-Commissariat à la Protection nationale tout incident ayant eu un impact significatif sur la sécurité et la pérennité du fonctionnement de l'infrastructure.

(4) La structure des plans de sécurité et de continuité de l'activité des infrastructures critiques est fixée par règlement grand-ducal.

**Art. 9.** En cas d'imminence ou de survenance d'une crise, le propriétaire ou opérateur d'une infrastructure critique, qui doit être, sauf en cas d'extrême urgence, dûment averti, est tenu de donner libre accès aux agents du Haut-Commissariat à la Protection nationale aux installations, locaux, terrains, aménagements faisant partie de l'infrastructure visée par la présente loi et les règlements à prendre en vue de son application.

Les actions de visite ou de contrôle entreprises sur place respectent le principe de proportionnalité.

Les dispositions reprises aux alinéas qui précèdent ne sont pas applicables aux locaux qui servent à l'habitation.

## Chapitre 4*bis* – La stratégie nationale en matière de sécurité des réseaux et des systèmes d'information

**Art. 9*bis*.** Le Haut-Commissariat à la Protection nationale élabore une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information, qui porte, en particulier, sur les points suivants :

a) les objectifs et les priorités de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information ;

b) un cadre de gouvernance permettant d'atteindre les objectifs et les priorités de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information, prévoyant notamment les rôles et les responsabilités des organismes publics et des autres acteurs pertinents ;

c) l'inventaire des mesures en matière de préparation, d'intervention et de récupération, y compris la coopération entre les secteurs public et privé ;

d) un aperçu des programmes d'éducation, de sensibilisation et de formation en rapport avec la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information ;

e) un aperçu des plans de recherche et de développement en rapport avec la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information ;

f) un plan d'évaluation des risques permettant d'identifier les risques ;

g) une liste des différents acteurs concernés par la mise en œuvre de la stratégie nationale en matière de sécurité des réseaux et des systèmes d'information.

## Chapitre 4*ter* – L'Agence nationale de la sécurité des systèmes d'information

**Art. 9*ter*.** (1) Dans sa fonction d'ANSSI, le Haut-Commissariat à la Protection nationale a pour missions :

a) de définir la politique générale de sécurité de l'information de l'État ;

b) de définir, en concertation avec les administrations et services de l'État, les politiques et lignes directrices de sécurité de l'information pour les domaines spécifiques, d'émettre des recommandations d'implémentation y relatives et d'assister les entités au niveau de l'implémentation des mesures proposées ;

c) de définir, en concertation avec les administrations et services de l'État, une approche de gestion des risques, en vue de constituer un plan d'évaluation et d'identification des risques concernant la sécurité de l'information et d'accompagner, à leur demande, les entités dans l'analyse et la gestion des risques ;

d) de conseiller l'Institut national d'administration publique, respectivement, à leur demande, les administrations et services de l'État dans la définition d'un programme de formation dans le domaine de la sécurité de l'information ;

e) de promouvoir la sécurité de l'information par le biais de mesures de sensibilisation ;

f) d'assurer la fonction d'autorité TEMPEST en veillant à la conformité des réseaux et systèmes d'information classifiés aux stratégies et lignes directrices TEMPEST et en approuvant les contre-mesures TEMPEST pour les installations et les produits destinés à protéger des pièces classifiées jusqu'à un certain niveau de classification dans leur environnement opérationnel.

(2) Les missions de l'ANSSI peuvent être élargies, à leur demande, à d'autres autorités publiques, aux établissements publics, ainsi qu'aux infrastructures critiques.

## Chapitre 4*quater* – Le CERT Gouvernemental

**Art. 9*quater*.** (1) Dans sa fonction de CERT Gouvernemental, le Haut-Commissariat à la Protection nationale a pour missions :

a) de constituer le point de contact unique dédié au traitement des incidents de sécurité d'envergure affectant les réseaux et les systèmes d'information des administrations et services de l'État ;

b) d'assurer un service de veille, de détection, d'alerte et de réaction aux attaques informatiques et aux incidents de sécurité d'envergure affectant ces réseaux et systèmes d'information ;

c) d'assurer la fonction de centre national de traitement des urgences informatiques, dénommé CERT National, en

1. opérant comme le point de contact officiel national pour les CERTs nationaux et gouvernementaux étrangers ;
2. opérant comme le point de contact officiel national pour la collecte et la distribution d'informations relatives aux incidents de sécurité qui concernent les réseaux et systèmes d'information implantés au Luxembourg ;

3. relayant les informations collectées aux CERTs sectoriels en charge de la cible d'une attaque ou à défaut de CERT sectoriel, directement à la cible.

d) d'assurer la fonction de centre militaire de traitement des urgences informatiques, dénommé CERT Militaire, en

1. opérant comme le point de contact officiel national pour les CERTs militaires étrangers ;
2. assurant un service de veille, de détection, d'alerte et de réaction aux attaques informatiques et aux incidents de sécurité d'envergure affectant les réseaux et les systèmes de communication et de traitement de l'information de l'armée à partir du territoire du Grand-Duché ;
3. opérant, à partir du territoire du Grand-Duché, une équipe d'intervention spécialisée capable de prendre en charge la réponse aux incidents de sécurité d'envergure liés à ces systèmes de communication et de traitement de l'information.

(2) Les missions du CERT Gouvernemental peuvent être élargies, à leur demande, à d'autres autorités publiques, aux établissements publics, ainsi qu'aux infrastructures critiques.

(3) Pour l'exécution de ses missions, le CERT Gouvernemental bénéficie de la part des administrations et services de l'État de toute la collaboration nécessaire.

## Chapitre 4*quinquies* – Le Service de la communication de crise

**Art. 9*quinquies*.** Dans sa fonction de Service de la communication de crise, le Haut-Commissariat à la Protection nationale a pour missions :

a) de coordonner la communication de crise avant, pendant et après des situations de crise pouvant frapper le territoire national, par l'intermédiaire des médias, l'internet et les réseaux sociaux ;

b) d'effectuer une communication préventive et pédagogique en sensibilisant les médias et le public sur les questions relevant de la protection du pays, de ses sites sensibles et de sa population ;

c) de créer et de maintenir des contacts étroits et réguliers avec les services de communication de crise étrangers.

## Chapitre 5 – Le personnel du Haut-Commissariat à la Protection nationale

**Art. 10.** La nomination ~~à la fonction de Haut-Commissaire à la Protection nationale~~aux fonctions de Haut-Commissaire à la Protection nationale et de Haut-Commissaire à la Protection nationale adjoint se fait par arrêté grand-ducal sur proposition du membre du Gouvernement ayant dans ses attributions la Protection nationale.

Le Haut-Commissaire à la Protection nationale est responsable de la gestion de l'administration. Il en est le chef hiérarchique. Il est assisté d'un Haut-Commissaire à la Protection nationale adjoint auquel il peut déléguer certaines de ses attributions et qui le remplace en cas d'absence.

**Art. 11.** (1) Le cadre du personnel comprend un Haut-Commissaire à la Protection nationale, un Haut-Commissaire à la Protection nationale adjoint et des fonctionnaires des différentes catégories de traitement telles que prévues par la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État.

(2) Le cadre du personnel peut être complété par des employés et salariés de l'État dans la limite des crédits budgétaires.

~~Le détachement des agents appelés au Haut-Commissariat à la Protection nationale se fait par arrêté du membre du Gouvernement ayant dans ses attributions la Protection nationale avec l'accord du ministre du ressort duquel relève l'agent en cause.~~

**Art. 12.** Un règlement grand-ducal détermine les modalités d'organisation des stages, des examens de fin de stage et des examens de promotion pour le personnel du Haut-Commissariat à la Protection nationale.

## Chapitre 6 – Dispositions spéciales

**Art. 13.** En cas d'imminence ou de survenance d'une crise, le Conseil de Gouvernement assure la coordination des mesures de réquisition prévues par la loi du 8 décembre 1981 sur les réquisitions en

cas de conflit armé, de crise internationale grave ou de catastrophe, par le titre V de la loi modifiée du 31 mai 1999 portant création d'un corps de police grand-ducale et d'une inspection générale de la police, ainsi que par le chapitre 4 de la loi communale modifiée du 13 décembre 1988.

**Art. 14.** Le Haut-Commissariat à la Protection nationale peut traiter les données personnelles nécessaires à l'exécution de la mission définie à l'article 3. Ces traitements sont soumis à la procédure d'autorisation préalable de la Commission nationale pour la protection des données telle que prévue à l'article 14 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

## Chapitre 7 – Dispositions modificatives, transitoires et spéciales

**Art. 15.** (1) Les fonctionnaires et employés visés à l'article 11 et relevant de la rubrique «Administration générale» telle qu'énoncée à l'article 12 de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État, en service auprès du Haut-Commissariat à la Protection nationale au moment de l'entrée en vigueur de la présente loi, sont intégrés dans le cadre du personnel du Haut-Commissariat à la Protection nationale aux grade et échelon atteints au moment de l'entrée en vigueur de la présente loi.

(2) Les fonctionnaires détachés au Haut-Commissariat à la Protection nationale au moment de la mise en vigueur de la présente loi, intégrés dans le cadre du personnel du Haut-Commissariat à la Protection nationale, et qui d'après la législation en vigueur dans leur service d'origine au moment de leur détachement avaient une perspective de carrière plus favorable pour l'accès aux différentes fonctions de leur carrière, conservent leurs anciennes possibilités d'avancement.

**Art. 15*bis*.** (1) Le personnel de l'ANSSI, du CERT Gouvernemental et du SCC est repris dans le cadre du personnel du Haut-Commissariat à la Protection nationale.

(2) Les fonctionnaires disposant d'un grade de substitution ou d'une majoration d'échelon pour postes à responsabilités particulières avant la reprise continuent à en bénéficier par dépassement du nombre limite fixé en vertu des dispositions de l'article 16 de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État aussi longtemps qu'ils restent titulaires d'un poste à responsabilités particulières. Il en est de même des employés qui bénéficient d'une telle majoration sur la base de l'article 29 de la loi modifiée du 25 mars 2015 déterminant le régime et les indemnités des employés de l'État.

**Art. 16.** À l'article 16 de la loi du 23 juillet 1952 concernant l'organisation militaire, telle qu'elle a été modifiée dans la suite, il est inséré un nouveau point libellé comme suit: « 2) les officiers, les sous-officiers et les caporaux de carrière employés par ordre du Gouvernement auprès du Haut-Commissariat à la Protection nationale. »

L'actuel point 2) devient le point 3).

**Art. 17.** La loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État est modifiée comme suit :

(1) à l'article 12, paragraphe 1er, alinéa 7, point 11°, les termes « de Haut-Commissaire à la Protection nationale, » sont insérés avant les termes « et de directeur de différentes administrations » ;

(2) dans l'annexe A « Classification des fonctions », Catégorie de traitement A, Groupe de traitement A1, Sous-groupe à attributions particulières, il est ajouté la mention « Haut-Commissaire à la Protection nationale » au grade 17 ;

(3) au paragraphe b) de l'article 17, il est inséré, à la suite des termes « inspecteur général de la sécurité dans la Fonction publique », la mention « Haut-Commissaire à la Protection nationale ».

**Art. 18.** La loi du 8 décembre 1981 sur les réquisitions en cas de conflit armé, de crise internationale grave ou de catastrophe, est modifiée comme suit :

1) au chapitre Ier, article 1er, dernière phrase, il est ajouté en fin de phrase: « ou d'une crise, au sens de la loi portant création d'un Haut-Commissariat à la Protection nationale et modifiant a) la loi

modifiée du 23 juillet 1952 concernant l'organisation militaire, b) la loi du 8 décembre 1981 sur les réquisitions en cas de conflit armé, de crise internationale grave ou de catastrophe, c) la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, d) la loi modifiée du 25 juin 2009 sur les marchés publics, e) la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'État, f) la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État ».

2) au chapitre IV, article 8 b) *in fine*, il est ajouté: « 5) Les agents du Haut-Commissariat à la Protection nationale ».

**Art. 19.** Au chapitre III, article 14 (1) de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, il est ajouté *in fine* un point (h) :

« (h) les traitements concernant la prévention et la gestion de crises conformément à l'article 14 de la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale et modifiant a) la loi modifiée du 23 juillet 1952 concernant l'organisation militaire, b) la loi du 8 décembre 1981 sur les réquisitions en cas de conflit armé, de crise internationale grave ou de catastrophe, c) la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, d) la loi modifiée du 25 juin 2009 sur les marchés publics, e) la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'État, f) la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État ».

**Art. 20.** À l'article 1er de la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'État, telle qu'elle a été modifiée dans la suite, il est inséré un tiret supplémentaire libellé comme suit: « – de Haut-Commissaire à la Protection nationale. »

**Art. 21.** Au livre Ier, titre III, chapitre III, article 8 (1) de la loi modifiée du 25 juin 2009 sur les marchés publics, il est ajouté *in fine* un point l) :

«l) pour les marchés de la protection nationale :

a) pour les fournitures ou services qui sont déclarés secrets ;

b) pour les fournitures ou services nécessaires à la protection des intérêts vitaux ou des besoins essentiels de tout ou partie du pays ou de la population, et en particulier les fournitures ou services relatifs à la prévention et la gestion de crises ;

c) pour les fournitures d'effets d'équipement et de matériel d'intervention ainsi que d'effets personnels de protection et de sécurité des membres des unités d'intervention. »

**Art. 22.** La référence à la présente loi pourra se faire sous une forme abrégée en utilisant les termes « loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale ».

**Art. 23.** La présente loi entre en vigueur le premier jour du deuxième mois qui suit sa publication au Mémorial.

Mandons et ordonnons que la présente loi soit insérée au Mémorial pour être exécutée et observée par tous ceux que la chose concerne.

*

## LOI MODIFIEE DU 9 DECEMBRE 2005

### déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'Etat (extraits)

**Art. 1er.** La nomination aux fonctions dirigeantes dans les administrations et services de l'Etat est faite pour une durée renouvelable de sept ans, sans préjudice des dispositions légales particulières prévoyant une nomination à durée déterminée pour un autre terme et sans préjudice des dispositions légales relatives à la limite d'âge de mise à la retraite.

Par fonction dirigeante au sens de la présente loi on entend les fonctions :

– de directeur général ou de directeur général adjoint,
– de président, à l'exception des fonctions de président du Conseil arbitral des assurances sociales,
– de directeur, de directeur adjoint ou de sous-directeur,
– d'administrateur général ou de premier conseiller de Gouvernement,
– de ministre plénipotentiaire,
– de chef d'état-major, de chef d'état-major adjoint ou de commandant du centre militaire,
– de premier inspecteur de la sécurité sociale ou de premier conseiller de direction,
– de commissaire, de commissaire de Gouvernement ou de commissaire de Gouvernement adjoint,
– de secrétaire général et
– d'inspecteur général ou d'inspecteur général adjoint,
– de médecin-chef de division de l'Administration des Services médicaux du Secteur public,
– de premier conseiller de légation
– de représentant permanent auprès de l'Union européenne
– ~~de Haut-Commissaire à la Protection nationale.~~ de Haut-Commissaire à la Protection nationale et de Haut-Commissaire à la Protection nationale adjoint,
– de directeur central
– commissaire à la langue luxembourgeoise.
– le médiateur au maintien, à l'inclusion et à l'intégration scolaires

classées aux grades 16, 17, 18, S1, F16, F17 et E6 à E8 figurant à l'annexe A, Classification des fonctions, de la loi du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat.

Les fonctionnaires nommés à une fonction dirigeante énumérée à l'alinéa 2 doivent faire preuve des compétences de direction et d'encadrement requises pour l'exercice de leurs fonctions. Ces compétences font l'objet d'un système d'appréciation dont les conditions et modalités sont fixées par voie de règlement grand-ducal.

Les fonctionnaires visés à l'alinéa qui précède peuvent être révoqués de leurs fonctions s'il existe un désaccord fondamental et persistant avec le Gouvernement sur l'exécution de leurs missions ou s'ils se trouvent dans une incapacité durable d'exercer leurs fonctions.

Le chef d'état-major de l'Armée, le directeur général de la Police et le directeur du Service de Renseignement peuvent être révoqués de leurs fonctions avec effet immédiat et en dehors des conditions prévues à l'alinéa précédent.

[…]

*

## LOI MODIFIEE DU 27 FEVRIER 2011
### sur les réseaux et les services de communications électronique (extraits)

[…]

**Art. 5.** (1) En cas de conflit armé, ~~de crise internationale grave ou de catastrophe~~ de crise internationale grave, de catastrophe ou de crise au sens de la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, le Gouvernement peut, pour une période limitée et dans le plus strict respect du principe de proportionnalité, réquisitionner tous les réseaux de communications électroniques établis sur le territoire du Grand-Duché, ainsi que les équipements y connectés, ou interdire en tout ou en partie la fourniture d'un service de communications électroniques. Cette réquisition ou cette interdiction ne donneront lieu à aucun dédommagement de la part de l'Etat.

(2) Sans préjudice du paragraphe (1), en cas ~~de catastrophe majeure~~ de catastrophe majeure ou de crise au sens de la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, afin de maintenir l'accès aux services d'urgence tout en assurant la communication entre les services d'urgence, les autorités et les services de radiodiffusion auprès du public, des conditions temporaires spécifiques d'utilisation des réseaux et des services de communications électroniques peuvent être décidées par le Gouvernement en Conseil.

En cas d'extrême urgence, cette décision peut être prise par un membre du Gouvernement qui en informera le Gouvernement en Conseil à la première occasion possible.

(3) Sans préjudice du paragraphe (1), en cas de menace immédiate grave pour l'ordre public, la sécurité publique ou la santé publique, des conditions temporaires spécifiques d'utilisation des réseaux et des services de communications électroniques peuvent être décidées par le Gouvernement en Conseil.

En cas d'extrême urgence, cette décision peut être prise par un membre du Gouvernement qui en informera le Gouvernement en Conseil à la première occasion possible.

(4) Il est institué un « comité national des communications » composé de vingt représentants au maximum, issus des ministères et organismes de l'Etat, qui assiste et conseille le Gouvernement dans l'élaboration des conditions d'utilisation mentionnées aux paragraphes précédents.

Les membres du comité sont nommés par le Premier Ministre, Ministre d'Etat sur proposition des ministres respectifs.

(5) Un descriptif général de ces conditions arrêtées par le Gouvernement est transmis aux entreprises notifiées par l'intermédiaire de l'Institut.

[…]

*

## LOI MODIFIEE DU 25 MARS 2015
### fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat (extraits)

[…]

**Art. 12. Rubrique « Administration générale » :**

[…]

Pour le sous-groupe à attributions particulières mentionné sous d), le classement des fonctions est défini comme suit:

[…]

8° Les fonctions de commissaire du Gouvernement adjoint du commissariat du Gouvernement chargé de l'instruction disciplinaire, de commissaire du Gouvernement adjoint à la protection des données auprès de l'État, de conseiller à la cour des comptes, de conseiller de Gouvernement première classe, de directeur adjoint de différentes administrations, d'inspecteur général adjoint de la sécurité dans

la Fonction publique, de directeur fonctionnel du Corps grand-ducal d'incendie et de secours, de Haut-Commissaire à la Protection nationale adjoint et de vice-président du Conseil arbitral des assurances sociales sont classées au grade 16.

[…]

**Art. 17.** Bénéficient d'une majoration d'échelon pour fonctions dirigeantes, les fonctionnaires nommés à une des fonctions désignées ci-après:

a) Pour le secrétaire général au ravitaillement, la valeur des différents échelons du grade 13 est augmentée de 20 points indiciaires.

b) Pour les fonctionnaires énumérés ci-après, la valeur des différents échelons de leurs grades respectifs est augmentée de 25 points indiciaires:

«directeurs généraux, directeurs généraux adjoints, directeurs, premier conseiller de légation, présidents, ministres plénipotentiaires, administrateurs généraux, commissaires, commissaire du Gouvernement adjoint chargé de l'instruction disciplinaire, colonel-chef d'état-major, inspecteur général adjoint de la sécurité dans la Fonction publique, inspecteur général de la sécurité dans la Fonction publique, Haut-Commissaire à la Protection nationale, Haut-Commissaire à la Protection nationale adjoint, lieutenant-colonel/chef d'état-major adjoint, lieutenant-colonel/commandant du centre militaire, vice-présidents, directeurs adjoints, inspecteur général de la Police inspecteur général adjoint de la police, directeurs centraux de la police, médecins-directeurs, représentant permanent auprès de l'Union européenne, secrétaire du Grand-Duc, secrétaire général du Conseil d'Etat, secrétaire général du Conseil économique et social, secrétaire général du département des affaires étrangères. Bénéficient de la même mesure le médecin dirigeant chargé de la direction de la division de la santé au travail du secteur public et le médecin dirigeant de la division de la médecine de contrôle du secteur public, ainsi que les fonctionnaires classés aux grades M5, M6, M7 et S1. »

Toutefois, l'agent bénéficiaire d'une majoration d'échelon pour fonctions dirigeantes ne peut pas bénéficier d'une majoration d'échelon pour postes à responsabilités particulières.

[…]

**Art. 22.** […]

(2) Une prime d'astreinte de 12 points indiciaires est allouée:

a) aux agents de la catégorie de traitement A, groupes de traitement A1 et A2, sous-groupe policier et sous-groupe à attributions particulières de la Police et de l'Inspection générale de la Police de la rubrique « Armée, Police et Inspection générale de la Police »;

b) aux agents de la catégorie de traitement B, groupe de traitement B1 du sous-groupe policier de la rubrique « Armée, Police et Inspection générale de la Police »;

c) aux agents de la catégorie de traitement D, groupe de traitement D2, sous-groupe technique nommés aux fonctions d'agent des domaines et de surveillant des domaines non visés au paragraphe 1er;

d) aux agents de la catégorie de traitement C, groupe de traitement C1, sous-groupe à attributions particulières, de la rubrique « Armée, Police et Inspection générale de la Police ».

e) aux agents du cadre supérieur et du cadre moyen des pompiers professionnels du Corps grand-ducal d'incendie et de secours, tels que définis aux articles 51 et 52 de la loi du 27 mars 2018 portant organisation de la sécurité civile ;

f) au directeur général, ainsi qu'aux directeurs fonctionnels du Corps grand-ducal d'incendie et de secours.

(3) Bénéficient d'une prime d'astreinte les fonctionnaires dont le service, de par sa nature et son organisation réglementaire, comporte, soit périodiquement soit à intervalles réguliers, du travail exécuté:

a) la nuit, entre vingt-deux et six heures;

b) les samedis, dimanches ou jours fériés légaux ou réglementaires, entre six et vingt-deux heures.

(4) Pour le fonctionnaire dont le service implique en permanence du travail alternant par équipes successives, le travail presté pendant les périodes définies au paragraphe 3 ci-dessus donne lieu à une prime d'astreinte dont la valeur horaire est fixée à 0,60 point indiciaire.

Pour le fonctionnaire périodiquement ou occasionnellement astreint à du service pendant les mêmes périodes, les heures de travail effectivement prestées donnent lieu à une prime d'astreinte dont la valeur horaire est fixée à 0,48 point indiciaire.

Les modalités d'application et le calcul de la prime prévue au présent paragraphe sont fixés par règlement grand-ducal.

(5) Une prime d'astreinte peut être allouée par règlement grand-ducal aux fonctionnaires de la catégorie de traitement D de la rubrique « Administration générale » chargés du service de concierge, impliquant la surveillance dans les bâtiments dans les administrations et services de l'Etat; la prime tient compte de l'affectation et des aménagements de l'immeuble ou de l'installation dont le fonctionnaire a la surveillance. Le montant de cette prime ne pourra dépasser 22 points indiciaires sauf si les heures de service sont prestées par équipes successives auquel cas il y a lieu d'appliquer les paragraphes 3 et 4 qui précèdent.

(6) Une prime d'astreinte ne pouvant dépasser la valeur de 22 points indiciaires peut être allouée par règlement grand-ducal aux fonctionnaires d'administrations exerçant tant des devoirs de police se situant en dehors de leur activité principale, que des attributions de police générale.

Ce règlement déterminera les catégories de fonctionnaires bénéficiant de la prime et en fixera le montant suivant l'importance des attributions exercées, pour autant que les bénéficiaires ne touchent pas de prime plus élevée par application des paragraphes 3 ou 4 ci-dessus.

(7) Une prime d'astreinte d'une valeur de 12 points indiciaires, indépendante de celle dont question au paragraphe 4 ci-dessus, est allouée aux fonctionnaires des différentes fonctions de facteur, énumérées à l'article 12, en raison de sujétions particulières auxquelles ces fonctionnaires sont soumis. Cette prime peut être cumulée avec celle spécifiée au paragraphe 4 ci-dessus. Toutefois, le montant des deux primes cumulées ne pourra dépasser la valeur de 22 points indiciaires. Si le montant de la prime visée au paragraphe 4 ci-dessus dépasse déjà à lui seul 22 points indiciaires, seule cette prime est payée.

(8) Une prime d'astreinte d'une valeur de 12 points indiciaires peut être allouée au personnel du cadre civil de la Police grand-ducale soumis à une obligation de permanence ou de présence. Cette prime est attribuée par décision du ministre du ressort et sur proposition du directeur général de la Police grand-ducale.

(9) Une prime d'astreinte d'une valeur de douze points indiciaires peut être allouée au personnel du cadre civil de l'Inspection générale de la Police soumis à une obligation de permanence ou de présence. Cette prime est attribuée par décision du ministre du ressort et sur proposition de l'inspecteur général de la Police.

(10) Une prime d'astreinte d'une valeur de 12 points indiciaires peut être allouée au personnel du Haut-Commissariat à la Protection nationale soumis à une obligation de permanence ou de présence. Cette prime est attribuée par décision du ministre du ressort et sur proposition du Haut-Commissaire à la Protection nationale.

[…]

*

ANNEXES

[…]

**B2) Allongements**

1. Pour les fonctionnaires de la catégorie de traitement A, groupe de traitement A1, sous-groupe à attributions particulières de la rubrique « Administration générale » nommés à la fonction de commissaire du Gouvernement adjoint du commissariat du Gouvernement chargé de l'instruction disciplinaire, de commissaire du Gouvernement adjoint à la protection des données auprès de l'État, de conseiller de Gouvernement première classe, de directeur adjoint, d'inspecteur général adjoint de la sécurité dans

la fonction publique, de médecin-dentiste dirigeant, de Haut-Commissaire à la Protection nationale adjoint ou de vice-président du Conseil arbitral des assurances sociales le grade 16 est allongé d'un douzième et treizième échelon ayant respectivement les indices 575 et 594.

[…]

*

## LOI MODIFIEE DU 8 AVRIL 2018
## sur les marchés publics (extraits)

[…]

**Art. 20. Conditions de recours à la procédure restreinte sans publication d'avis et à la procédure négociée**

(1) En cas de procédure restreinte sans publications d'avis, les pouvoirs adjudicateurs adressent une demande d'offre à un nombre limité d'opérateurs économiques, au gré du pouvoir adjudicateur, dans les cas prévus à l'alinéa 3 et au paragraphe 3. Le nombre minimum de candidats invités à soumissionner est de trois.

En cas de procédure négociée, les pouvoirs adjudicateurs consultent les opérateurs économiques de leur choix et négocient les conditions de marché avec un ou plusieurs d'entre eux.

Il peut être recouru soit à la procédure restreinte sans publication d'avis, soit à la procédure négociée dans les cas suivants :

a) lorsque le montant total du marché à conclure n'excède pas une somme à déterminer par règlement grand-ducal ; cette somme peut varier selon les différents corps de métier en présence, mais sans qu'elle ne puisse dépasser 8 000 euros hors TVA, valeur cent de l'indice des prix à la consommation au 1er janvier 1948, adapté conformément à l'article 160.

   S'il s'agit de dépenses à engager au cours d'une même année et pour un même objet et que ces dépenses aient été prévisibles, il devra être tenu compte de l'ensemble des dépenses portant sur des travaux, fournitures et services de nature identique ou similaire commandés à un même opérateur économique.

b) en présence d'offres non conformes ou inacceptables à la suite du recours à une procédure ouverte ou à une procédure restreinte avec publication d'avis ou lorsque aucune offre n'a été déposée, pour autant que la passation du contrat soit urgente ; sinon l'exception est applicable sous les mêmes conditions, mais après une seconde procédure ouverte ou une seconde procédure restreinte avec publication d'avis ;

c) pour des travaux, fournitures et services qui sont réalisés à des fins de recherche, d'expérimentation, d'étude ou de mise au point ;

d) dans des cas exceptionnels, lorsqu'il s'agit de travaux, fournitures et services dont la nature ou les aléas ne permettent pas une fixation préalable et globale des prix ;

e) pour les travaux, fournitures et services dont l'exécution, pour des raisons techniques, artistiques, scientifiques ou tenant à la protection de droits d'exclusivité, ne peut être confiée qu'à un opérateur économique déterminé;

f) dans la mesure du strictement nécessaire, lorsque l'urgence impérieuse résultant d'événements imprévisibles ne permet pas de respecter les délais exigés par les autres procédures. Les circonstances invoquées pour justifier l'urgence impérieuse ne doivent en aucun cas être imputables aux pouvoirs adjudicateurs ;

g) Pour de nouveaux travaux ou services consistant dans la répétition de travaux ou de services similaires confiés à l'opérateur économique adjudicataire du marché initial par les mêmes pouvoirs adjudicateurs, à condition que ces travaux ou ces services soient conformes à un projet de base et que ce projet ait fait l'objet d'un marché initial passé selon une procédure dans le cadre de laquelle un appel à concurrence a été publié. Le projet de base précise l'étendue des travaux ou services supplémentaires possibles, et les conditions de leur attribution.

   La possibilité de recourir à cette procédure est indiquée dès la mise en concurrence du premier projet et le montant total envisagé pour les travaux ou les services supplémentaires est pris en considération par les pouvoirs adjudicateurs pour l'application de l'article 52.

Il n'est possible de recourir à cette procédure que pendant une période de trois ans suivant la conclusion du marché initial.

h) dans le cadre de marchés publics de fournitures, pour des livraisons complémentaires effectuées par le fournisseur initial et destinées soit au renouvellement partiel de fournitures ou d'installations, soit à l'extension de fournitures ou d'installations existantes, lorsque le changement de fournisseur obligerait le pouvoir adjudicateur à acquérir des fournitures ayant des caractéristiques techniques différentes entraînant une incompatibilité ou des difficultés techniques ou d'entretien disproportionnées ;

i) dans le cadre de marchés publics de fournitures, pour les fournitures cotées et achetées à une bourse des matières premières ;

j) lorsqu'il s'agit de travaux, fournitures et services dont les prix sont en fait soustraits au jeu normal de la concurrence ou s'il s'agit de services rémunérés suivant un barème officiel ;

k) pour les marchés de travaux, de fournitures, et de services de la Police grand-ducale :
   - pour les prestations occasionnées par le déplacement et le séjour de personnel policier à l'étranger dans le cadre des missions policières ;
   - lorsque la sécurité du personnel engagé est directement menacée ;
   - pour les fournitures d'effets d'habillement et d'équipement militaire destinés à être revendus au cadre.

l) pour les marchés de travaux, de fournitures, et de services de l'Armée :
   - si le secret militaire l'exige ;
   - pour les besoins d'une standardisation des matériels et équipements ;
   - pour les travaux, fournitures et services occasionnés par le déplacement et le séjour d'unités militaires à l'étranger ;
   - pour l'acquisition de denrées alimentaires périssables lors de séjours à l'étranger ;
   - pour les fournitures d'effets d'habillement et d'équipement militaire destinés à être revendus au cadre.

m) pour les marchés de la protection nationale :
   - pour les fournitures ou services qui sont déclarés secrets ;
   - pour les fournitures ou services nécessaires à la protection des intérêts vitaux ou des besoins essentiels de tout ou partie du pays ou de la population, et en particulier les fournitures ou services relatifs à la prévention et la gestion de crises ;
   - pour les travaux de réfection de dommages résultant d'une crise telle que définie à l'article 2, point 2, de la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, et pour autant que la réparation soit urgente ;
   - pour les fournitures d'effets d'équipement et de matériel d'intervention ainsi que d'effets personnels de protection et de sécurité des membres des unités d'intervention.

(2) Il peut être recouru à la procédure négociée dans les cas suivants :

a) pour les marchés à conclure par les pouvoirs adjudicateurs compétents pour l'Armée, la Police grand-ducale, l'Administration des Douanes et Accises et pour les services de secours, pour des besoins de standardisation des équipements et du matériel d'intervention ainsi que des effets personnels de protection et de sécurité des membres des unités d'intervention ;

b) pour les marchés publics de services, lorsque le marché considéré fait suite à un concours dont les règles sont à instituer par voie de règlement grand-ducal, et est, en vertu des règles prévues dans le cadre du concours, attribué au lauréat ou à un des lauréats de ce concours ; dans ce dernier cas, tous les lauréats du concours sont invités à participer aux négociations ;

c) pour les achats d'opportunité, lorsqu'il est possible d'acquérir des fournitures en profitant d'une occasion particulièrement avantageuse qui s'est présentée dans une période de temps très courte et pour lesquelles le prix à payer est considérablement plus bas que les prix normalement pratiqués sur les marchés ainsi que pour les achats de fournitures dans des conditions particulièrement avantageuses soit auprès d'un fournisseur cessant définitivement ses activités soit auprès de curateurs ou liquidateurs, d'une faillite ou d'un concordat judiciaire ;

d) pour les marchés qui servent à la mise en œuvre de moyens techniques particuliers et confidentiels de recherche, d'investigation et de sécurisation lorsque la protection des intérêts essentiels de l'État l'exige.

(3) Il peut être recouru soit à la procédure restreinte sans publication d'avis, soit à la procédure négociée lorsque le montant total du marché se situe entre le seuil fixé par voie de règlement grand-ducal et quatorze mille euros hors TVA, valeur cent de l'indice des prix à la consommation au 1er janvier 1948, adapté conformément à l'article 160, sous condition que le pouvoir adjudicateur, dans l'hypothèse d'une procédure restreinte sans publication d'avis, invite au moins trois candidats à soumissionner, et dans l'hypothèse d'une procédure négociée, admet au moins trois candidats aux négociations, à condition chaque fois qu'il y ait un nombre suffisant de candidats appropriés.

(4) Les marchés publics pour les services sociaux et pour d'autres services spécifiques visés à l'article 76 et à l'article 148, et qui tombent dans le champ d'application du présent Livre, peuvent en toute hypothèse être attribués par voie de procédure négociée.

(5) Les marchés qui sont exclus du champ d'application du Livre II conformément aux articles 55 à 61 et qui relèvent du champ d'application du présent Livre, peuvent en toute hypothèse être attribués par voie de procédure négociée.

(6) Les marchés qui sont exclus du champ d'application du Livre III conformément aux articles 100 à 115 et qui relèvent du champ d'application du présent Livre, peuvent en toute hypothèse être attribués par voie de procédure négociée.

[…]

**Art. 159. Commission des soumissions**

(1) Il est institué, auprès du ministre ayant dans ses attributions les travaux publics, une Commission des soumissions, dont les membres sont nommés par arrêté du Gouvernement en conseil.

La commission est assistée d'un service administratif.

La composition de la commission, son mode de saisine et de fonctionnement, ainsi que celui du service administratif lui joint, de même que les indemnités des membres et du personnel administratif, sont déterminés par voie de règlement grand-ducal.

(2) La Commission des soumissions a pour mission :

a) de veiller à ce que les dispositions légales, réglementaires et contractuelles en matière de marchés publics soient strictement observées par les pouvoirs adjudicateurs et les entités adjudicatrices, ainsi que par les adjudicataires ;

b) d'instruire les réclamations ;

c) d'assumer toute mission consultative relative aux marchés publics ;

d) de donner son avis à tout pouvoir adjudicateur ou entité adjudicatrice qui le demande, relativement aux marchés publics à passer ou conclus ;

e) d'exécuter les tâches spécifiques lui confiées par la présente loi et ses règlements d'exécution.

(3) Si un pouvoir adjudicateur se propose de recourir, pour un marché estimé, hors TVA, à plus de 50 000 euros, valeur cent de l'indice des prix à la consommation au 1er janvier 1948, adapté conformément à l'article 160, à une procédure restreinte sans publication d'avis ou à une procédure négociée sans publication préalable, il doit au préalable solliciter l'avis de la Commission des soumissions.

En cas de survenance d'une crise telle que définie à l'article 2, point 2, de la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, le Haut-Commissariat à la Protection nationale est exempté du respect de l'obligation visée à l'alinéa qui précède, pour la passation de marchés en application des articles 20, paragraphe 1er, lettre f), 64, paragraphe 2, lettre c), et 124, lettre d), dès lors que les conditions d'application de ces dispositions sont remplies.

*

## FICHE FINANCIERE

(article 79 de la loi modifiée du 8 juin 1999 sur le Budget, la Comptabilité et la Trésorerie de l'Etat)

Les frais supplémentaires engendrés par le projet de loi sont de 58.000 EUR par an. Ils proviennent du fait qu'une prime d'astreinte d'une valeur de 12 points indiciaires est allouée aux membres du personnel du Haut-Commissariat à la Protection nationale qui sont soumis à une obligation de permanence ou de présence (actuellement 20 personnes).

*

## FICHE D'EVALUATION D'IMPACT

**Coordonnées du projet**

| | |
|---|---|
| **Intitulé du projet :** | **Projet de loi modifiant**<br>**1° la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale,**<br>**2° la loi modifiée du 9 décembre 2005 déterminant les conditions et modalités de nomination de certains fonctionnaires occupant des fonctions dirigeantes dans les administrations et services de l'Etat,**<br>**3° la loi modifiée du 27 février 2011 sur les réseaux et les services de communications électroniques,**<br>**4° la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'Etat et**<br>**5° la loi modifiée du 8 avril 2018 sur les marchés publics** |
| **Ministère initiateur :** | **Ministère d'Etat** |
| **Auteur(s) :** | **Elisabeth Wirion** |
| **Téléphone :** | **247-88912** |
| **Courriel :** | **elisabeth.wirion@hcpn.etat.lu** |
| **Objectif(s) du projet :** | **Le projet vise à inclure l'Agence nationale de la sécurité des systèmes d'information, le Centre de traitement des urgences informatiques et le Service de la communication de crise dans la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale.**<br>**Accessoirement, l'avant-projet adapte la loi sur les réseaux et services communications électroniques et la loi sur les marchés publics à la terminologie et aux missions décrites dans la loi-cadre du HCPN.**<br>**Finalement, il est procédé à des ajustements ponctuels de la loi-cadre du HCPN en matière de personnel.** |
| **Autre(s) Ministère(s)/Organisme(s)/Commune(s)impliqué(e)(s) :**<br>**Ministère de la Fonction publique, Ministère de la Mobilité et des Travaux publics, Centre des technologies de l'information de l'État, Institut luxembourgeois de régulation, Service des médias et des communications** | |
| **Date :** | **13/07/2020** |

**Mieux légiférer**

1. Partie(s) prenante(s) (organismes divers, citoyens, …) consultée(s) : Oui ☒ Non ☐
   Si oui, laquelle/lesquelles : Ministère de la Fonction publique, Ministère de la Mobilité et des Travaux publics, Centre des technologies de l'information de l'État, Institut luxembourgeois de régulation, Service des médias et des communications
   Remarques/Observations : Les entités consultées se sont montrées d'accord avec le projet.

2. Destinataires du projet :
   – Entreprises/Professions libérales : Oui ☐ Non ☒
   – Citoyens : Oui ☐ Non ☒
   – Administrations : Oui ☐ Non ☒

3. Le principe « Think small first » est-il respecté ? Oui ☐ Non ☐ N.a.[1] ☒
   (c.-à-d. des exemptions ou dérogations sont-elles prévues suivant la taille de l'entreprise et/ou son secteur d'activité ?)
   Remarques/Observations :

4. Le projet est-il lisible et compréhensible pour le destinataire ? Oui ☒ Non ☐
   Existe-t-il un texte coordonné ou un guide pratique, mis à jour et publié d'une façon régulière ? Oui ☒ Non ☐
   Remarques/Observations : Des textes législatifs coordonnés accompagnent le projet de loi.

5. Le projet a-t-il saisi l'opportunité pour supprimer ou simplifier des régimes d'autorisation et de déclaration existants, ou pour améliorer la qualité des procédures ? Oui ☐ Non ☒
   Remarques/Observations :

6. Le projet contient-il une charge administrative[2] pour le(s) destinataire(s) ? (un coût imposé pour satisfaire à une obligation d'information émanant du projet ?) Oui ☐ Non ☒
   Si oui, quel est le coût administratif[3] approximatif total ? (nombre de destinataires x coût administratif par destinataire)

7. a) Le projet prend-il recours à un échange de données inter-administratif (national ou international) plutôt que de demander l'information au destinataire ? Oui ☐ Non ☐ N.a. ☒
      Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il ?
   b) Le projet en question contient-il des dispositions spécifiques concernant la protection des personnes à l'égard du traitement des données à caractère personnel[4] ? Oui ☐ Non ☐ N.a. ☒

---

1 N.a. : non applicable.

2 Il s'agit d'obligations et de formalités administratives imposées aux entreprises et aux citoyens, liées à l'exécution, l'application ou la mise en oeuvre d'une loi, d'un règlement grand-ducal, d'une application administrative, d'un règlement ministériel, d'une circulaire, d'une directive, d'un règlement UE ou d'un accord international prévoyant un droit, une interdiction ou une obligation.

3 Coût auquel un destinataire est confronté lorsqu'il répond à une obligation d'information inscrite dans une loi ou un texte d'application de celle-ci (exemple: taxe, coût de salaire, perte de temps ou de congé, coût de déplacement physique, achat de matériel, etc.).

4 Loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (www.cnpd.lu)

Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il ?

8. Le projet prévoit-il :
   – une autorisation tacite en cas de non réponse de l'administration ? Oui ☐ Non ☐ N.a. ☒
   – des délais de réponse à respecter par l'administration ? Oui ☐ Non ☐ N.a. ☒
   – le principe que l'administration ne pourra demander des informations supplémentaires qu'une seule fois ? Oui ☐ Non ☐ N.a. ☒

9. Y a-t-il une possibilité de regroupement de formalités et/ou de procédures (p.ex. prévues le cas échéant par un autre texte) ? Oui ☐ Non ☐ N.a. ☒
   Si oui, laquelle :

10. En cas de transposition de directives communautaires, le principe « la directive, rien que la directive » est-il respecté ? Oui ☐ Non ☐ N.a. ☒
    Sinon, pourquoi ?

11. Le projet contribue-t-il en général à une :
    a) simplification administrative, et/ou à une Oui ☐ Non ☒
    b) amélioration de la qualité réglementaire ? Oui ☐ Non ☒
    Remarques/Observations :

12. Des heures d'ouverture de guichet, favorables et adaptées aux besoins du/des destinataire(s), seront-elles introduites ? Oui ☐ Non ☐ N.a. ☒

13. Y a-t-il une nécessité d'adapter un système informatique auprès de l'Etat (e-Government ou application back-office) ? Oui ☐ Non ☒
    Si oui, quel est le délai pour disposer du nouveau système ?

14. Y a-t-il un besoin en formation du personnel de l'administration concernée ? Oui ☐ Non ☐ N.a. ☒
    Si oui, lequel ?
    Remarques/Observations :

**Egalité des chances**

15. Le projet est-il :
    – principalement centré sur l'égalité des femmes et des hommes ? Oui ☐ Non ☒
    – positif en matière d'égalité des femmes et des hommes ? Oui ☐ Non ☒
      Si oui, expliquez de quelle manière :
    – neutre en matière d'égalité des femmes et des hommes ? Oui ☒ Non ☐
      Si oui, expliquez pourquoi :
    – négatif en matière d'égalité des femmes et des hommes ? Oui ☐ Non ☒
      Si oui, expliquez de quelle manière :

16. Y a-t-il un impact financier différent sur les femmes et les hommes ? Oui ☐ Non ☐ N.a. ☒
    Si oui, expliquez de quelle manière :

**Directive « services »**

17. Le projet introduit-il une exigence relative à la liberté d'établissement soumise à évaluation[5] ? Oui ☐ Non ☐ N.a. ☒

Si oui, veuillez annexer le formulaire A, disponible au site Internet du Ministère de l'Economie et du Commerce extérieur :

www.eco.public.lu/attributions/dg2/d_consommation/d_march_int_rieur/Services/index.html

18. Le projet introduit-il une exigence relative à la libre prestation de services transfrontaliers[6] ? Oui ☐ Non ☐ N.a. ☒

Si oui, veuillez annexer le formulaire B, disponible au site Internet du Ministère de l'Economie et du Commerce extérieur :

www.eco.public.lu/attributions/dg2/d_consommation/d_march_int_rieur/Services/index.html

5 Article 15, paragraphe 2 de la directive « services » (cf. Note explicative, p. 10-11)

6 Article 16, paragraphe 1, troisième alinéa et paragraphe 3, première phrase de la directive « services » (cf. Note explicative, p. 10-11)

Impression: CTIE – Division Imprimés et Fournitures de bureau