



Textes coordonnés

Les modifications prévues par le présent projet de loi dans les textes de loi repris ci-dessous sont marquées en gras.

A. Loi modifiée du 20 avril 2009 portant création du Centre des technologies de l'information de l'État

(EXTRAITS)

(...)

Art. 2.

Le centre a pour mission :

- a) la promotion et l'organisation de façon rationnelle et coordonnée de l'automatisation des administrations de l'État notamment en ce qui concerne la collecte, la transmission et le traitement des données ;
- b) l'assistance des différentes administrations de l'État dans l'exécution des travaux courants d'informatique, ainsi que la gestion des systèmes de communication fixes et mobiles ;
- c) la gestion des équipements électroniques, informatiques et de sécurité appropriés à l'accomplissement de ses attributions ;
- d) l'administration du réseau informatique commun et de la messagerie électronique de l'État ;
- e) la sécurité de l'informatique et le respect des dispositions de la loi relative à la protection des personnes à l'égard du traitement des données à caractère personnel, dans les limites de ses attributions ;
- f) la production et la personnalisation de documents administratifs sécurisés et le traitement des données biométriques y relatives ;
- g) l'acquisition et la gestion d'équipements informatiques et bureautiques et de machines de bureau pour les administrations de l'État ;
- h) la gestion d'un centre de support destiné aux utilisateurs internes et externes des systèmes d'informations gérés par le centre ;
- i) l'élaboration et la tenue à jour d'une cartographie des processus des administrations de l'État et de leur interopérabilité ;
- j) le support organisationnel des administrations de l'État et leur accompagnement dans leurs projets de réorganisation ;
- k) la recherche de synergies entre les différentes administrations de l'État et l'optimisation de leurs échanges d'informations ;
- l) la coordination de la présence Internet des administrations de l'État ;
- m) la mise en place et l'exploitation des plateformes d'échange avec les citoyens et les entreprises ;
- n) la mise en place et l'exploitation de plateformes de collaboration reliant l'ensemble des agents de l'État ;
- o) la mise en place et la coordination d'un réseau de guichets physiques régionaux qui offrent aux citoyens un point de contact unique quelles que soient leurs démarches administratives ;

- p) la mise à disposition d'une base de connaissances regroupant l'ensemble des attributions de l'État et accessible à travers les différents canaux de services publics ;
- q) l'acquisition, l'entreposage et la diffusion de fournitures de bureau, de manuels et publications scolaires et d'imprimés destinés aux administrations de l'État ;
- r) l'impression, l'entreposage et la diffusion des documents parlementaires et d'ouvrages publiés par les administrations de l'État ;
- s) la transmission des informations officielles entre les gouvernements, les organismes internationaux et les administrations de l'État, selon les directives de sécurité en vigueur ;
- t) ~~la planification, la mise en place, la gestion, l'exploitation et l'assurance de la disponibilité des systèmes de communication et d'information classifiés permettant la consultation politique et l'échange d'informations au profit du Gouvernement~~ l'exercice de la fonction d'autorité opérationnelle, ci-après « AO », compétente pour :
 - 1° la planification, la mise en place, la gestion, l'exploitation et l'assurance de la disponibilité des systèmes d'information et de communication, ci-après « SIC », permettant l'échange d'informations classifiées au profit du Gouvernement, y compris l'acquisition des produits essentiels à la protection des SIC ;
 - 2° l'élaboration des documents relatifs à la sécurité et la formation des utilisateurs des SIC, propres à chaque SIC ;
 - 3° la mise en œuvre et la gestion des mesures de sécurité et de l'assurance de l'information classifiée, propres à chaque SIC ; et
 - 4° la participation à la sélection des mesures et des dispositifs de sécurité TEMPEST et la veille à ce qu'ils soient installés et entretenus de manière sûre en coopération avec l'autorité nationale TEMPEST.

Par dérogation à l'alinéa 1^{er}, le Service de renseignement de l'État assure la fonction d'AO des SIC qu'il opère exclusivement.

Le centre désigne les entités publiques ou privées de droit luxembourgeois pouvant assumer elles-mêmes la fonction d'AO sous condition qu'elles en aient fait la demande, que cette demande soit justifiée par les besoins de la réalisation de projets d'intérêt public et qu'elles puissent justifier par rapport à l'ANS le respect des mesures de protection applicables aux SIC.

Si l'entité concernée ne respecte plus les conditions visées à l'alinéa précédent, l'ANS en informe le centre qui révoque la désignation ;

- u) ~~l'exercice, dans le cadre de ces attributions, de la fonction d'Autorité nationale de distribution, responsable de la gestion du matériel cryptographique des organismes nationaux et internationaux cryptographique, ci-après « ADC », compétente pour la centralisation de la gestion et de la distribution de matériel cryptographique communiqué aux entités, aux organisations internationales ou aux États tiers ou reçu de ceux-ci.~~ Par dérogation à l'alinéa 1^{er}, le Service de renseignement de l'État assure la gestion et la distribution du matériel cryptographique liées aux SIC qu'il opère exclusivement.

Le centre désigne les entités publiques ou privées de droit luxembourgeois comme pouvant assumer elles-mêmes la gestion et la distribution du matériel cryptographique sous condition qu'elles en aient fait la demande, que cette demande soit justifiée par les besoins

de la réalisation de projets d'intérêt public et qu'elles puissent justifier par rapport au centre le respect des mesures de protection applicables au matériel cryptographique.

Si les conditions visées à l'alinéa précédent ne sont plus remplies, le centre révoque la désignation ;

- v) l'exercice de la fonction ~~de Bureau d'ordre central qui est l'entité nationale responsable d'organiser la réception, la comptabilisation, la distribution et la destruction des pièces classifiées d'autorité nationale centrale de réception et de communication des pièces classifiées de niveau « TRÈS SECRET », assurée par le bureau d'ordre central, ci-après « BOC ».~~

Le BOC est compétent :

1° pour la réception et la diffusion centralisées des pièces classifiées de niveau « TRÈS SECRET » communiquées ou reçues en dehors d'un SIC ; et

2° pour la supervision de l'enregistrement des pièces classifiées de niveau « CONFIDENTIEL » ou supérieur communiquées ou reçues en dehors d'un SIC ;

- w) la mise à la disposition du Gouvernement d'une infrastructure sécurisée et des ressources administratives, logistiques, de communications électroniques et de traitement de l'information nécessaires à la gestion de crises ;
- x) la mise à la disposition du Gouvernement d'un centre de conférences nationales et internationales ;
- y) l'opération du service courrier du Gouvernement ;
- z) l'exercice, ~~dans le cadre de ces attributions,~~ de la fonction d'Autorité d'agrément cryptographique, ~~chargée de veiller à ce que les produits cryptographiques soient conformes aux politiques de sécurité respectives en matière cryptographique ; d'évaluer et d'agréer les produits cryptographiques pour la protection des informations classifiées jusqu'à un certain niveau de classification dans leur environnement opérationnel ; de conserver et de gérer les données techniques relatives aux produits cryptographiques~~ compétente pour :
- 1° l'évaluation des produits cryptographiques pour la protection des pièces classifiées jusqu'au niveau de classification demandé dans le cadre d'une demande d'agrément ;
- 2° la délivrance, le renouvellement, la modification, la suspension et le retrait d'agréments de produits cryptographiques ; et
- 3° la veille de la conformité des produits cryptographiques aux politiques de sécurité applicables en matière cryptographique.

(...)

B. Loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État

(EXTRAITS)

(...)

Art. 2. – Organisation et contrôle hiérarchique

(1) Le SRE est placé sous l'autorité hiérarchique du membre du Gouvernement ayant le renseignement de l'État dans ses attributions, désigné ci-après « le ministre ».

(2) Le SRE accomplit ses missions conformément aux directives fixées par un Comité ministériel du renseignement sur proposition du ministre, composé de membres du Gouvernement, désigné ci-après le « Comité ».

Le Comité établit, sur proposition du ministre, la politique générale du renseignement et détermine les orientations des activités du SRE. Il définit en outre la politique en matière de protection des renseignements sensibles.

Le Comité surveille les activités du SRE.

(3) Sur proposition du ministre, le Conseil de Gouvernement désigne parmi les fonctionnaires de la carrière supérieure des administrations de l'État un fonctionnaire qui justifie de l'expérience adéquate pour l'exercice de la fonction comme délégué au SRE.

Le délégué au SRE qui doit être détenteur d'une habilitation de sécurité du niveau « TRÈS SECRET », a pour mission de surveiller le fonctionnement du SRE. Il fait régulièrement rapport au ministre.

Il assume la fonction de secrétaire auprès du Comité.

Il assiste aux réunions de direction du SRE et il peut prendre part à toute autre réunion de service au sein du SRE.

Il est régulièrement tenu au courant des activités du SRE par le directeur. Aucun secret ne peut lui être opposé.

Il dispose d'une compétence propre d'investigation et de contrôle au sein du SRE, sans pour autant pouvoir s'immiscer dans l'exécution courante des missions dudit service prévues à l'article 3 qui reste de la seule responsabilité du directeur du SRE.

(4) Le directeur est responsable de la gestion de l'administration. Il en est le chef hiérarchique.

Il est assisté de **deux trois** directeurs adjoints auxquels il peut déléguer certaines de ses attributions et qui le remplacent en cas d'absence.

Le SRE comprend la direction ainsi que différentes divisions dont les attributions sont déterminées par le directeur, sous réserve de l'approbation du ministre.

Le directeur arrête les détails d'organisation et les modalités de fonctionnement du SRE.

(...)

Art. 18. – Direction

Pour être nommé aux fonctions de directeur ou de directeur adjoint du SRE, le candidat doit remplir les conditions d'accès aux fonctions administratives de la carrière supérieure auprès des administrations de l'État prévue par la loi modifiée du 16 avril 1979 fixant le statut général des fonctionnaires de l'État et avoir l'honorabilité professionnelle nécessaire ainsi que l'expérience adéquate pour l'exercice de ces fonctions.

Le directeur et les directeurs adjoints doivent justifier d'une habilitation de sécurité du niveau « TRÈS SECRET ».

~~Le directeur ou l'un des directeurs adjoints doit être titulaire d'un diplôme de master sanctionnant un cycle d'études universitaires complet en droit.~~ Deux membres de la direction au moins, dont celui dont les attributions comportent la gestion journalière de l'Autorité nationale de sécurité, doivent être titulaires d'un diplôme de master sanctionnant un cycle d'études universitaires complet en droit.

Art. 19. – Cadre du personnel du SRE

(1) Le cadre du personnel comprend un directeur, ~~deux~~ trois directeurs adjoints et des fonctionnaires des différentes catégories de traitement telles que prévues par la loi 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 fonctionnaires stagiaires, des employés et des salariés dans la limite des crédits budgétaires.

(3) Le SRE communique chaque année à la commission de contrôle parlementaire les demandes et les prévisions d'effectifs ainsi que le nombre d'effectifs engagés.

(4) Dans la limite des crédits budgétaires le SRE peut recourir à des experts qui concourent à l'accomplissement de ses missions sur base de contrats de prestation de services à conclure par le ministre.

(...)

C. Loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale

(EXTRAITS)

(...)

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 oeuvre 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.

(1bis) Le Haut-Commissariat à la Protection nationale est encore chargé des missions suivantes :

- a) attributions dans sa fonction d'Agence nationale de la sécurité des systèmes d'information, ci-après « ANSSI » ;
- b) attributions dans sa fonction de Centre de traitement des urgences informatiques, ci-après « CERT Gouvernemental » ;
- c) attributions dans sa fonction de Service de la communication de crise, ci-après « SCC ».

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

- a) de contribuer à la mise en œuvre de la politique générale de sécurité de l'information de l'État ;
- b) de contribuer à la mise en œuvre, en concertation avec les administrations et services de l'État, des politiques et lignes directrices de sécurité de l'information portant sur les domaines de la politique générale de sécurité de l'information de l'État et des nouvelles technologies de l'information et de la communication ;
- c) d'émettre des recommandations d'implémentation des politiques et lignes directrices de sécurité de l'information et d'assister les administrations et services de l'État au niveau de l'implémentation des mesures proposées ;
- d) 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 administrations et services de l'État dans l'analyse et la gestion des risques ;
- e) 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 ;
- f) de promouvoir la sécurité de l'information par le biais de mesures de sensibilisation ;
- g) de conseiller, à leur demande, les établissements publics et les infrastructures critiques en matière de sécurité des réseaux et systèmes d'information et des risques y liés ;

h) 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 pour :~~

1° veiller à la conformité des systèmes d'information et de communication, tels que définis dans la loi du JJ.MM.AAAA relative à la protection des pièces classifiées, aux stratégies et lignes directrices TEMPEST ;

2° l'approbation des mesures destinées à prévenir la compromission des pièces classifiées dans les lieux et dans les SIC par des émissions électromagnétiques non-intentionnelles (« mesures de sécurité TEMPEST ») ; et

3° la délivrance, la modification, la suspension et le retrait de certificats relatifs à la protection des SIC contre la compromission par des émissions électromagnétiques non-intentionnelles.

(1quater) 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 et, à leur demande, des établissements publics et des infrastructures critiques ;

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 les réseaux et systèmes d'information des administrations et services de l'État et, à leur demande, des établissements publics et des infrastructures critiques ;

c) d'assurer la fonction de centre national de traitement des urgences informatiques, dénommé CERTNational, 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 d'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 réseaux et systèmes d'information.

Le Haut-Commissaire à la Protection nationale peut, dans l'intérêt de l'exécution des missions du CERT Gouvernemental, demander leur concours aux agents des administrations et services de l'État.

(1quinquies) 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.

(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.

D. Loi modifiée du 17 août 2018 relative à l'archivage

(EXTRAITS)

(...)

Art. 4

(1) Par dérogation au paragraphe 1^{er} de l'article 3, les ~~archives publiques~~ pièces classifiées conformément à la loi du ~~15 juin 2004 relative à la classification des pièces et aux habilitations de sécurité~~ JJ.MM.AAAA relative à la protection des pièces classifiées doivent être proposées au versement aux Archives nationales après avoir été déclassifiées et après expiration de la durée d'utilité administrative.

(2) Les producteurs ou détenteurs d'archives publiques suivants conservent et gèrent eux-mêmes leurs archives publiques conformément aux principes de la présente loi :

1. la Chambre des députés ;
2. le Conseil d'État ;
3. les juridictions luxembourgeoises ;
4. la Cour grand-ducale ;
5. le Médiateur ;
6. la Cour des comptes ;
7. les établissements publics de l'État ;
8. l'Institut Grand-Ducal.

Au cas où ces producteurs ou détenteurs d'archives publiques ne peuvent pas conserver eux-mêmes leurs archives publiques, les Archives nationales conservent leurs archives publiques après expiration de la durée d'utilité administrative.

(3) L'Archevêché de Luxembourg, les Consistoires de l'Église protestante et de l'Église protestante réformée du Luxembourg, le Consistoire administratif de l'Église protestante du Luxembourg, le Consistoire israélite, l'Église anglicane du Luxembourg, l'Église orthodoxe au Luxembourg, les Églises orthodoxes hellénique, roumaine, serbe et russe établies au Luxembourg, la Shoura, assemblée de la Communauté musulmane du Grand-Duché de Luxembourg, le Fonds de gestion des édifices religieux et autres biens relevant du culte catholique ne sont pas soumis aux dispositions de la présente loi. Au cas où ils ne peuvent pas conserver eux-mêmes leurs archives publiques, ils les versent après expiration de la durée d'utilité administrative aux Archives nationales qui les conservent conformément aux principes de la présente loi et de ses règlements d'exécution. Sur demande, les organismes visés bénéficient des conseils de la part des Archives nationales.

(4) Les communes, les syndicats de communes et les établissements publics des communes ne sont pas soumis aux dispositions de la présente loi à l'exception des dispositions des chapitres IX et X et conservent eux-mêmes leurs archives conformément à la loi communale modifiée du 13 décembre 1988. L'État peut conclure des contrats de coopération avec les communes et les établissements publics des communes concernant leurs archives. Les contrats de coopération sont élaborés à partir d'un contrat de coopération type dont le contenu et les modalités sont définis par voie de règlement grand-ducal.

La conclusion de ces contrats avec les communes et les établissements publics des communes et leur exécution au nom et pour le compte de l'État relèvent de la compétence conjointe du ministre de la Culture et du ministre de l'Intérieur.

À défaut de contrat de coopération, les communes et les établissements publics des communes informent par écrit le directeur des Archives nationales avant toute destruction de leurs archives après l'expiration de leur durée d'utilité administrative. En cas d'opposition à la destruction de la part du directeur des Archives nationales, les archives en question sont versées aux Archives nationales.

Ils peuvent détruire leurs archives à défaut de réponse du directeur des Archives nationales dans un délai de trois mois.

(...)