Projet de loi

relative à la rétention des données à caractère personnel et portant modification:

1° **du Code de procédure pénale ;**
2° **de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques ; et**
3° **de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat**

I. – Texte du projet de loi

Art. 1er. Le Code de procédure pénale est modifié comme suit :

1° A la suite de l'article 24-2 du Code de procédure pénale, il est inséré un article 24-3 nouveau, libellé comme suit :

« Art. 24-3. (1) Pour les besoins de la recherche, de la constatation et de la poursuite d'infractions pénales qui emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement, et dans le seul but de permettre, en tant que de besoin, la mise à disposition des autorités judiciaires d'informations, le procureur d'État peut, dans l'exercice de ses fonctions, ordonner, par une décision écrite et motivée, le concours des opérateurs de télécommunications ou des fournisseurs d'un service de communications électroniques pour procéder à la conservation des données relatives au trafic et à la localisation, générées ou traitées par eux dans le cadre de la fourniture des services de communications concernés, qu'il juge nécessaires.

L'obligation de conserver inclut la conservation des données relatives aux appels téléphoniques infructueux lorsque ces données sont générées ou traitées, en ce qui concerne les données de la téléphonie, ou journalisées, en ce qui concerne les données de l'internet, dans le cadre de la fourniture des services de communications concernés. Un règlement grand-ducal détermine les catégories de données relatives au trafic susceptibles de pouvoir servir à la recherche, à la constatation et à la poursuite d'infractions visées ci-dessus. Ce règlement peut également déterminer les formes et les modalités suivant lesquelles les données visées sont à mettre à la disposition des autorités judiciaires.

La décision écrite et motivée mentionne :

a) L'infraction qui fait l'objet de l'ordre ;
b) L'indication précise d'un ou de plusieurs des éléments suivants : la ou les personnes, les moyens de communication ou les lieux qui font l'objet de la conservation ;
c) La durée de conservation des données, qui ne peut excéder six mois. Ce délai peut être prolongé par écrit.

En cas d'urgence, la conservation peut être ordonnée verbalement. L'ordre doit être confirmé dans les plus brefs délais dans la forme prévue à l'alinéa 3.

(2) Les données sont détruites lorsque la durée de conservation prend fin, à l'exception des données auxquelles on a pu légalement accéder et qui ont été préservées.

(3) Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

Toute personne qui refuse de prêter son concours technique aux réquisitions visées dans cet article, est punie d'une amende de 1.250 à 125.000 euros. »

2° L'article 48-27 du même code est remplacé comme suit :

« Art. 48-27. (1) Dans le cadre de l'enquête pour crime ou délit ou de l'instruction préparatoire, le procureur d'État ou le juge d'instruction peut, par une décision motivée et écrite, en requérant au besoin le concours d'un opérateur de télécommunications ou d'un fournisseur d'un service de communications électroniques, procéder ou faire procéder sur la base de toutes données détenues par lui sur base de l'article 10*ter*, paragraphe 1er, de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques à :

1° l'identification de l'abonné ou de l'utilisateur habituel d'un service de communication électronique ou du moyen de communication électronique utilisé ;

2° l'identification des services de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée.

La motivation reflète le caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête ou d'instruction.

(2) Dans le cadre de l'enquête pour crime ou délit ou de l'instruction préparatoire et si les faits emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement, le procureur d'État ou le juge d'instruction peut, par une décision motivée et écrite, en requérant au besoin le concours d'un opérateur de télécommunications ou d'un fournisseur d'un service de communications électroniques, procéder ou faire procéder sur la base de toutes données détenues par lui sur base de l'article 10*ter*, paragraphe 2, de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques à l'identification de l'utilisateur d'une adresse IP.

(3) Lorsqu'il existe une nécessité urgente de prévenir une atteinte grave à la vie, à la liberté ou à l'intégrité physique d'une personne ou lorsqu'il est impératif que les autorités qui procèdent à l'enquête agissent immédiatement pour éviter de compromettre sérieusement une procédure pénale, les officiers de police judiciaire visés à l'article 10 peuvent, avec l'accord oral et préalable du procureur d'État ou du juge d'instruction, et par une décision motivée et écrite requérir les données visées aux paragraphes 1er et 2. Ils communiquent cette décision motivée et écrite ainsi que les informations recueillies dans les vingt-quatre heures au procureur d'État ou au juge d'instruction et motivent par ailleurs l'extrême urgence.

(4) Les dispositions des paragraphes 1er à 3 sont à observer à peine de nullité.

(5) Chaque opérateur de télécommunications et chaque fournisseur d'un service de communications électroniques communique les informations qui ont été demandées dans les meilleurs délais.

Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation est punie conformément à l'article 458 du Code pénal.

Toute personne qui refuse de prêter son concours technique aux réquisitions visées dans cet article, est punie d'une amende de 1.250 à 125.000 euros. »

3° L'article 67-1 du même code est remplacé comme suit :

« Art. 67-1. (1) Lorsque le juge d'instruction estime qu'il existe des circonstances qui rendent le repérage de télécommunications ou des communications électroniques ou la localisation de l'origine ou de la destination de télécommunications ou des communications électroniques nécessaire à la manifestation de la vérité, et si les faits emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement, il peut faire procéder, en requérant au besoin le concours technique de l'opérateur de télécommunications et/ou du fournisseur d'un service de communications électroniques:

1. au repérage des données d'appel de moyens de télécommunication ou de communications électroniques à partir desquels ou vers lesquels des appels sont adressés ou ont été adressés, y inclus le repérage des adresses IP;
2. à la localisation de l'origine ou de la destination de télécommunications ou des communications électroniques.

Dans les cas visés à l'alinéa 1, pour chaque moyen de télécommunication ou de communication électronique dont les données d'appel sont repérées ou dont l'origine ou la destination de la télécommunication ou de la communication électronique est localisée, le jour, l'heure, la durée et, si nécessaire, le lieu de la télécommunication ou de la communication électronique sont indiqués et consignés dans un procès-verbal.

Le juge d'instruction indique les circonstances de fait de la cause qui justifient la mesure dans une ordonnance motivée qu'il communique au procureur d'Etat.

Il précise la durée durant laquelle elle pourra s'appliquer, cette durée ne pouvant excéder un mois à dater de l'ordonnance, sans préjudice de renouvellement.

(2) Chaque opérateur de télécommunications et chaque fournisseur des services concernés communique les informations qui ont été demandées dans les meilleurs délais.

Toute personne qui, du chef de sa fonction, a connaissance de la mesure ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

Toute personne qui refuse de prêter son concours technique aux réquisitions visées dans cet article, est punie d'une amende de 100 à 5.000 euros.

(3) La personne dont un moyen de télécommunication ou de communication électronique a fait l'objet de la mesure prévue au paragraphe 1er est informée de la mesure ordonnée au cours même de l'instruction et en tout cas au plus tard dans les 12 mois qui courent à partir de la date de l'ordonnance. Toutefois ce délai de 12 mois ne s'applique pas lorsque la mesure a été ordonnée dans une instruction pour des faits qui se situent dans le cadre ou en relation avec une association ou une organisation criminelle au sens

des articles 322 à 324*quater* du Code pénal, ou qui se situent dans le cadre ou en relation avec le terrorisme au sens des articles 135-1 à 135-6, 135-9 et 135-11 à 135-16 du Code pénal, ou au sens de l' article 10, alinéa 1 de la loi modifiée du 19 février 1973 concernant la vente de substances médicamenteuses et la lutte contre la toxicomanie.

La requête en nullité doit être produite sous peine de forclusion, dans les conditions prévues à l'article 126 du Code de procédure pénale.

Lorsque les mesures de repérage de télécommunications ou de communications électroniques ordonnées par le juge d'instruction n'ont donné aucun résultat, les données obtenues seront retirées du dossier de l'instruction et détruites dans la mesure où elles concernent des personnes non inculpées. »

Art. 2. La loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques est modifiée comme suit :

1° L'article 2, point (b) de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, est remplacé par le texte suivant :

« (b) « consentement »: toute manifestation de volonté libre, spécifique, éclairée et univoque par laquelle la personne concernée ou son représentant légal, judiciaire ou statutaire accepte, par une déclaration ou par un acte positif clair, que les données à caractère personnel la concernant fassent l'objet d'un traitement; »

2° L'article 3, paragraphe 1er, alinéa 2 de la même loi, est remplacé comme suit :

« Sous réserve des dispositions générales du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, les mesures visées ci-dessus, pour le moins:

- garantissent que seules des personnes autorisées peuvent avoir accès aux données à caractère personnel à des fins légalement autorisées,
- protègent les données à caractère personnel stockées ou transmises contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelles et le stockage, le traitement, l'accès et la divulgation non autorisés ou illicites, et
- assurent la mise en œuvre d'une politique de sécurité relative au traitement des données à caractère personnel. »

3° L'article 5 de la même loi est remplacé comme suit :

« Art. 5. Données relatives au trafic

(1) Tout fournisseur de services de communications électroniques ou opérateur qui traite des données relatives au trafic concernant les abonnés et les utilisateurs, est tenu de prendre toutes les dispositions nécessaires pour que de telles données soient effacées ou rendues anonymes dès lors qu'elles ne sont plus nécessaires à la transmission d'une communication ou aux traitements prévus par les dispositions des paragraphes 2 et 3, à l'exception des accès qui sont:

- ordonnés par les autorités judiciaires et par le comité ministériel du renseignement pour le Service de renseignement de l'Etat agissant dans le cadre des compétences leur attribuées par la loi pour sauvegarder la sécurité nationale, pour la lutte contre la criminalité grave et pour la prévention de menaces graves contre la sécurité publique, ou

- demandés par les organes compétents dans le but de régler des litiges notamment en matière d'interconnexion ou de facturation ».

(2) Les données relatives au trafic qui sont nécessaires en vue d'établir les factures des abonnés et aux fins des paiements d'interconnexion peuvent être traitées. Un tel traitement n'est possible que jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement et ne peut en tout état de cause dépasser 6 mois lorsque la facture a été payée et n'a pas fait l'objet de litige ou de contestation.

(3) Les données relatives au trafic peuvent être traitées en vue de commercialiser des services de communications électroniques ou de fournir des services à valeur ajoutée dans la mesure et pour la durée nécessaires à la fourniture ou à la commercialisation de ces services pour autant que le fournisseur d'un service de communications électroniques ou l'opérateur informe préalablement l'abonné ou l'utilisateur concerné des types de données relatives au trafic traitées, de la finalité et de la durée du traitement et que celui-ci ait donné son consentement, nonobstant son droit de s'opposer à tout moment à un tel traitement.

(4) Le traitement des données relatives au trafic effectué dans le cas des activités visées aux paragraphes 1er à 3 est restreint aux personnes agissant sous l'autorité du fournisseur de services ou de l'opérateur qui sont chargés d'assurer la facturation ou la gestion du trafic, répondre aux demandes de clientèle, détecter les fraudes, commercialiser les services de communications électroniques ou fournir un service à valeur ajoutée. Le traitement doit se limiter à ce qui est nécessaire à de telles activités.

(5) Quiconque contrevient aux dispositions des paragraphes 1er à 4 du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction. »

4° A la suite de l'article 5 de la même loi, il est inséré un article 5*bis* nouveau, libellé comme suit :

« Art. 5*bis*. (1) Pour les besoins de sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention de menaces graves contre la sécurité publique, tout fournisseur d'un service de communications électroniques ou opérateur est tenu de conserver les données relatives au trafic et à la localisation pour les zones géographiques visées au paragraphe 2, pendant six mois à partir de la date de la communication.

L'obligation de conserver inclut la conservation des données relatives aux appels téléphoniques infructueux lorsque ces données sont générées ou traitées et stockées, en ce qui concerne les données de la téléphonie, ou journalisées, en ce qui concerne les données de l'internet, dans le cadre de la fourniture des services de communications concernés. Pour l'application du présent paragraphe, une seule information de localisation est requise par communication ou appel.

Un règlement grand-ducal détermine les catégories de données relatives au trafic et les données de localisation susceptibles de pouvoir servir à la sauvegarde de la sécurité nationale, à la lutte contre la criminalité grave et à la prévention de menaces graves contre la sécurité publique.

(2) Les zones géographiques dans lesquelles sont conservées les données relatives au trafic et à la localisation sont les suivantes:

1° Les zones particulièrement exposées à des menaces pour la sécurité nationale ou à des risques élevés de préparation ou de commission d'actes de criminalité grave, à savoir :

a) Les lieux où sont commis, de manière répétée, des crimes ou délits dont les faits emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement ;
b) Les lieux qui par leur configuration sont de nature à favoriser la commission des crimes ou délits dont les faits emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement ;
c) Les alentours et abords des infrastructures où sont organisés régulièrement des évènements d'envergure nationale ou internationale ;
d) Les lieux qui par leur nature rassemblent un grand nombre de personnes.

L'étendue du périmètre de chaque zone géographique fait l'objet d'un arrêté grand-ducal, sur proposition de la commission consultative visée au paragraphe 4 au Haut-Commissariat à la protection nationale. L'arrêté grand-ducal est renouvelé tous les trois ans après évaluation du périmètre des zones géographiques de la commission consultative.

2° Si le niveau de la menace déterminé par le groupe de coordination en matière de lutte contre le terrorisme (GCT) selon l'évaluation visée au plan gouvernemental de vigilance nationale face aux menaces d'actions terroristes (plan "VIGILNAT") est au moins de niveau 3 et couvre l'ensemble du territoire, le Haut-Commissariat à la protection nationale informe immédiatement les opérateurs et fournisseurs de service concernés afin qu'ils procèdent à une conservation générale et indifférenciée des données relatives au trafic et à la localisation, sur l'ensemble du territoire.

(3) Les opérateurs conservent les données de trafic pour toutes les communications ou appels infructueux effectués à partir d'une zone géographique visée au paragraphe 2 ou vers une telle zone.

Lorsque l'utilisateur final se déplace pendant une communication électronique, l'opérateur ou le fournisseur de services concernés conserve les données relatives au trafic ou à la localisation pour autant que l'utilisateur final se trouve à un moment de la communication dans une zone visée au paragraphe 2.

Lorsque la technologie utilisée par l'opérateur ou le fournisseur de services concernés ne permet pas de limiter la conservation de données à une zone visée au paragraphe 2, il conserve les données nécessaires pour couvrir l'entièreté de la zone concernée tout en limitant la conservation de données en dehors de cette zone au strict nécessaire au regard de ses possibilités techniques.

(4) Il est créé une commission consultative ayant pour mission de présenter, tous les trois ans, un rapport d'évaluation au Haut-Commissariat à la protection nationale sur la mise en œuvre du présent article.

Le Haut-Commissariat à la protection nationale présente le rapport d'évaluation visé à l'alinéa 1er à la Chambre des députés.

La composition et les modalités de fonctionnement de la commission consultative sont fixées par règlement grand-ducal.

(5) Quiconque contrevient aux dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction. »

5° L'article 5-1 de la même loi, devenant l'article 5*ter* nouveau, est remplacé comme suit :

« Art. 5*ter.* (1) Les données conservées au titre des articles 5, 5*bis* et 9 de la présente loi par les autorités compétentes au sens de l'article 1er, paragraphe 1er, de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale sont soumises aux exigences prévues à l'article 28 de cette même loi.

(2) Les données sont détruites lorsque la durée de conservation prend fin, à l'exception des données auxquelles on a pu légalement accéder et qui ont été préservées. »

6° L'article 5-2 de la même loi, devenant l'article 5*quater* nouveau, est remplacé comme suit :

« Art. 5*quater.* (1) La Commission nationale pour la protection des données publie annuellement des statistiques sur la conservation de données au titre des articles 5 et 9.

A cet effet les fournisseurs de services de communications électroniques ou opérateurs conservent et continuent à la Commission nationale, sur demande de celle-ci, les informations comprenant notamment:

- les cas dans lesquels des informations ont été transmises aux autorités compétentes conformément à la législation nationale applicable,
- le laps de temps écoulé entre la date à partir de laquelle les données ont été conservées et la date à laquelle les autorités compétentes ont demandé leur transmission,
- les cas dans lesquels des demandes de données n'ont pu être satisfaites.

(2) Ces statistiques ne contiennent pas de données à caractère personnel. »

7° L'article 7, paragraphe 5*bis*, de la même loi est modifié comme suit :

« (5*bis*) En outre, en cas de communication d'urgence, au sens de l'article 2, point 38°, de la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques, vers le numéro d'urgence unique européen 112 ainsi que vers les numéros d'urgence déterminés par l'Institut luxembourgeois de régulation, les informations relatives à la localisation de l'appelant obtenues à partir de l'appareil mobile, si elles sont disponibles, sont mises à disposition sans tarder après l'établissement de la communication d'urgence au centre de réception des appels d'urgence le plus approprié, même lorsque l'appelant a désactivé la fonction de localisation. Ces informations sont à effacer après un délai de 24 heures au plus. »

8° L'article 9 de la même loi est modifié comme suit :

« Art. 9. Données de localisation autres que les données relatives au trafic

(1) Tout fournisseur de services de communications électroniques ou opérateur qui traite des données de localisation, autres que les données relatives au trafic, concernant les abonnés et les utilisateurs, est tenu de prendre toutes les dispositions nécessaires à ce que de telles données soient effacées ou rendues anonymes dès lors qu'elles ne sont plus nécessaires à la transmission d'une communication ou aux traitements prévus par les dispositions des paragraphes 2 et 3, à l'exception des accès qui sont ordonnés par les autorités judiciaires et par le comité ministériel du renseignement pour le Service de renseignement de l'Etat agissant dans le cadre des compétences leur attribuées par la loi pour sauvegarder la sécurité nationale, pour la lutte contre la criminalité grave et pour la prévention de menaces graves contre la sécurité publique.

(2) Tout fournisseur de services concernés ou opérateur ne peut traiter des données de localisation autres que les données relatives au trafic et concernant les abonnés ou les utilisateurs que si celles-ci ont été rendues anonymes ou moyennant le consentement de l'abonné ou de l'utilisateur, dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée et sous réserve des dispositions des paragraphes 1er, 3 et 4.

(3) Le fournisseur de services concernés et le cas échéant l'opérateur informe préalablement l'abonné ou l'utilisateur sur les types de données de localisation traitées, autres que les données relatives au trafic, sur la ou les finalité(s) et la durée de ce traitement ainsi que sur la transmission de ces données à des tiers en vue de la fourniture du service à valeur ajoutée. L'abonné ou l'utilisateur a la possibilité de retirer à tout moment son consentement pour le traitement des données de localisation autres que les données relatives au trafic.

Lorsque l'abonné ou l'utilisateur a donné son consentement au traitement des données de localisation autres que les données relatives au trafic, il doit garder la possibilité d'interdire temporairement, par un moyen simple et gratuit, le traitement de ces données pour chaque connexion au réseau ou pour chaque transmission de communication.

(4) Le traitement effectué des données de localisation, autres que les données relatives au trafic, dans le cas des activités visées aux paragraphes 1er à 3 est restreint aux personnes agissant sous l'autorité du fournisseur de services ou de l'opérateur ou du tiers qui fournit le service à valeur ajoutée. Le traitement doit se limiter à ce qui est nécessaire à de telles activités.

(5) Quiconque contrevient aux dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction. »

9° A la suite de l'article 10*bis* de la même loi, il est inséré un article 10*ter* nouveau, libellé comme suit :

« Art. 10*ter*. Conservation des données d'identification

(1) Tout fournisseur d'un service de communications électroniques ou opérateur est tenu de conserver les données suivantes, pour autant qu'il les traite ou les génère dans le cadre de la fourniture de ses services :

1° les données détenues par lui sur base de l'article 10*bis* de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques ;

2° les données de souscription de l'abonné ainsi que les données d'identification de l'utilisateur final ou le service de communications électroniques employé;

3° les adresses IP ayant servi à la souscription ou à l'activation du service de communication électronique ainsi que le port source de la connexion et l'horodatage;

4° l'identité internationale d'abonné mobile (IMSI);

5° l'identité internationale d'équipement mobile (IMEI).

L'opérateur ou le fournisseur des services concernés conserve les données visées à l'alinéa 1er pendant le délai fixé à l'article 10*bis*, paragraphe 7, alinéa 2.

(2) Pour les besoins de sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention de menaces graves contre la sécurité publique, tout opérateur de télécommunications ou fournisseur d'un service de communications électroniques est tenu de conserver l'adresse IP à la source de la connexion, l'horodatage de l'attribution ainsi que, en cas d'utilisation partagée d'une adresse IP de l'utilisateur final, les ports qui lui ont été attribués.

L'opérateur ou le fournisseur des services concernés conserve les données visées à l'alinéa 1er pour une durée de six mois après la fin de la session.

(3) Quiconque contrevient aux dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction. »

10° L'article 12 de la même loi est modifié comme suit :

« Art. 12. Commission nationale pour la protection des données

La Commission nationale pour la protection des données instituée par l'article 3 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données est chargée d'assurer l'application des dispositions de la présente loi et de ses règlements d'exécution sans préjudice de l'application de l'article 5 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données. »

Art. 3. La loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat est modifié comme suit :

1° A l'article 7, paragraphe 1er, de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat, le mot « y » est inséré entre les mots « données relatives au trafic, » et « compris

l'identification des correspondants » et le mot « télécommunications » est remplacé par les mots « communications électroniques ».

2° A la suite de l'article 7 de la même loi, il est inséré un article 7-1 nouveau, libellé comme suit :

« Art. 7-1. – *Injonction de conservation généralisée et indifférenciée des données relatives au trafic et à la localisation*

(1) Le SRE peut, dans l'intérêt de l'exercice de ses missions et lorsqu'il existe une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, requérir la collaboration ou le concours technique de l'opérateur de télécommunications, du fournisseur d'un service de communications électroniques, pour procéder à la conservation généralisée et indifférenciée des données relatives au trafic y compris l'identification des correspondants et de toutes les formes de communications ou à la localisation de l'origine ou de la destination de ces communications, générées ou traitées par eux dans le cadre de la fourniture des services de communications concernés.

(2) L'injonction de conservation visée au paragraphe 1er est ordonnée par le Comité sur demande écrite du directeur du SRE et après l'assentiment de la commission spéciale, selon la procédure inscrite à l'article 7, paragraphe 4.
Le SRE est autorisé à accéder aux données conservées conformément à l'article 7, paragraphe 2.

(3) L'injonction de conservation, qui mentionne la date à laquelle elle a été ordonnée ainsi que la durée de la conservation, est notifiée aux opérateurs et fournisseurs des services concernés qui font procéder sans retard à leur exécution.

(4) La durée de la conservation ne pourra se reporter qu'à une période maximale de six mois suivant la date à laquelle elle a été ordonnée, sans préjudice de la possibilité de prolongation en suivant la même procédure.

Le SRE met fin à l'injonction de conservation, lorsque la conservation n'est plus utile pour lutter contre la menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, ou lorsque cette menace a disparu. Lorsqu'il est mis fin avant l'échéance de la période autorisée, les opérateurs et fournisseurs des services concernés sont avertis dans les meilleurs délais.

(5) Une fois par mois, le directeur du SRE rapporte par écrit au Comité de l'évolution de la menace. Ce rapport met en évidence les éléments qui justifient soit le maintien de la conservation généralisée et indifférenciée, soit la fin de celle-ci.

(6) Toute personne qui, du chef de sa fonction, a connaissance de l'injonction prise en vertu du présent article ou y prête son concours, est tenue de garder le secret. Toute violation est punie conformément à l'article 458 du Code pénal.

Toute personne qui refuse de prêter son concours technique à l'injonction visée dans cet article, est punie d'une amende de 1.250 à 125.000 euros. »

3° A la suite de l'article 7-1 nouveau de la même loi, il est inséré un article 7-2 nouveau, libellé comme suit :

« Art. 7-2. – *Injonction de conservation ciblée des données relatives au trafic et à la localisation*

(1) Pour les besoins de sauvegarde de la sécurité nationale, le SRE peut, dans l'exercice de ses missions, requérir la collaboration ou le concours technique de l'opérateur de télécommunications, du fournisseur d'un service de communications électroniques ou du fournisseur de services de la société de l'information, pour procéder à:

1° la conservation rapide et immédiate des données relatives au trafic, y compris l'identification des correspondants et de toutes les formes de communications ou à la localisation de l'origine ou de la destination de ces communications, qui sont à sa disposition au moment de l'injonction;

2° la conservation de données relatives au trafic, y compris l'identification des correspondants et de toutes les formes de communications ou à la localisation de l'origine ou de la destination de ces communications, qu'il génère et traite à partir de l'injonction.

L'injonction de conservation est mise en œuvre sur demande écrite du directeur du SRE, suite à une demande motivée écrite de l'agent du SRE chargé des recherches et sous réserve des conditions et critères prévus à l'article 4. En cas d'urgence, la conservation peut être ordonnée verbalement par le directeur du SRE, à confirmer par écrit dans un délai de quarante-huit heures dans la forme prévue au paragraphe 2.

Le SRE est autorisé à accéder aux données conservées conformément à l'article 7, paragraphe 2.

(2) L'injonction de conservation est notifiée aux opérateurs et fournisseurs des services concernés qui font procéder sans retard à leur exécution et mentionne:

1° la nature des données de trafic et de localisation à conserver;

2° les personnes ou groupes de personnes, les zones géographiques, les moyens de communication et/ou le mode d'utilisation dont les données doivent être conservées;

3° la durée de conservation des données qui ne peut excéder six mois à compter de la date de l'injonction, sans préjudice de la possibilité de prolongation en suivant la même procédure.

(3) Le SRE met fin à l'injonction de conservation, lorsque la conservation n'est plus utile pour la sauvegarde de la sécurité nationale. Lorsqu'il est mis fin avant l'échéance de la période autorisée, les opérateurs et fournisseurs des services concernés sont avertis dans les meilleurs délais.

(4) Une fois par mois, le directeur du SRE rapporte par écrit au Comité des injonctions de conservation réalisées par le SRE avec les motifs spécifiques pour lesquels l'exercice des missions a exigé l'injonction.

(5) Toute personne qui, du chef de sa fonction, a connaissance de l'injonction prise en vertu du présent article ou y prête son concours, est tenue de garder le secret. Toute violation est punie conformément à l'article 458 du Code pénal.

Toute personne qui refuse de prêter son concours technique à l'injonction visée dans cet article, est punie d'une amende de 1.250 à 125.000 euros. »

Art. 4. Pour la première application de l'article 2, point 4°, la commission consultative transmet sa proposition de l'étendue du périmètre de chaque zone géographique au Haut-Commissariat à la protection nationale au plus tard le premier jour du troisième mois qui suit la publication de la présente loi au Journal officiel du Grand-Duché de Luxembourg.

Art. 5. La référence à la présente loi se fait sous la forme suivante : « Loi du jj.mm.aaaa relative à la rétention des données à caractère personnel. »

Art. 6. La présente loi entre en vigueur le quatrième jour de sa publication au Journal officiel du Grand-Duché de Luxembourg.

Par dérogation au paragraphe 1er, l'article 2, points 3°, 4° et 7°, entrent en vigueur le premier jour du douzième mois qui suit la publication de la présente loi au Journal officiel du Grand-Duché de Luxembourg.