IV. – TEXTES COORDONNES

1. Code de procédure pénale

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'Etat 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.

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 ~~**télécommunications**~~ **communications électroniques**, procéder ou faire procéder sur la base de toutes données détenues par lui sur base de l'article ~~**10*bis***~~ **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 ~~ces~~ **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 ~~du présent~~ **des** paragraphe**s 1er à 3** sont à observer à peine de nullité.

~~(2)~~ **(5)** Chaque opérateur de télécommunications et chaque fournisseur d'un service de ~~télécommunications~~ **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.

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 ~~télécommunications~~ **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 ~~**d'un service de télécommunications**~~ **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** ~~**(1)**~~ 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*** ~~**324*ter***~~ 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.

2. Loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

Art. 1er. Champ d'application

Sous réserve des dispositions générales concernant la protection des personnes à l'égard du traitement des données à caractère personnel ou régissant les réseaux et services de communications électroniques, les dispositions suivantes s'appliquent spécifiquement au traitement de ces données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux de communications publics

Art. 2. Définitions

Aux fins de la présente loi on entend par:

(a) «abonné»: une personne physique ou morale partie à un contrat avec une entreprise offrant des services de communications électroniques accessibles au public, pour la fourniture de tels services;

(b) «consentement»: toute manifestation de volonté libre, spécifique**, éclairée** et **univoque ~~informée~~** 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;

(c) «communication»: toute information échangée ou acheminée entre un nombre fini de parties au moyen d'un service de communications électroniques accessible au public à l'exception des informations qui sont acheminées dans le cadre d'un service de radiodiffusion au public par l'intermédiaire d'un réseau de communications électroniques sauf si et dans la mesure où un lien peut être établi entre l'information et l'abonné ou l'utilisateur identifiable qui la reçoit;

(d) «courrier électronique»: tout message sous forme de texte, de voix, de son ou d'image envoyé par un réseau de communications public qui peut être stocké dans le réseau ou dans l'équipement terminal du destinataire jusqu'à ce que ce dernier le récupère;

(e) «données relatives au trafic»: toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation;

(f) «données de localisation»: toutes les données traitées dans un réseau de communications électroniques ou par un service de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public;

(g) «Institut» : l'Institut Luxembourgeois de Régulation;

(h) «réseau de communications électroniques»: les systèmes de transmission et, le cas échéant, les équipements de commutation ou de routage et les autres ressources qui permettent l'acheminement de signaux par câble, par voie hertzienne, par moyen

optique ou par d'autres moyens électromagnétiques comprenant les réseaux satellitaires, les réseaux terrestres fixes (avec commutation de circuits ou de paquets, y compris l'Internet) et mobiles, les systèmes utilisant le réseau électrique, pour autant qu'ils servent à la transmission de signaux, les réseaux utilisés pour la radiodiffusion sonore et télévisuelle et les réseaux câblés de télévision, quel que soit le type d'information transmise;

(i) «réseau de communications public»: un réseau de communications électroniques utilisé entièrement ou principalement pour la fourniture de services de communications électroniques accessibles au public. Le fournisseur du réseau de communications public est dénommé ci-après «opérateur»;

(j) «service de communications électroniques»: un service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission de signaux sur les réseaux de communications électroniques, y compris les services de télécommunications et les services de transmission sur des réseaux utilisés pour la radiodiffusion, mais qui exclut les services consistant à fournir des contenus à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ces contenus; il ne comprend pas les services de la société de l'information qui ne consistent pas entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques. Le fournisseur de services de communications électroniques est dénommé ci-après «fournisseur de services»;

(k) «service à valeur ajoutée»: tout service qui exige le traitement de données relatives au trafic ou à la localisation, à l'exclusion des données qui ne sont pas indispensables pour la transmission d'une communication ou sa facturation;

(l) «utilisateur»: une personne physique ou morale qui utilise ou demande un service de communications électroniques accessible au public à des fins privées ou professionnelles sans être nécessairement abonnée à ce service ;

(m) « violation de données à caractère personnel»: une violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés de données à caractère personnel transmises, stockées ou traitées d'une autre manière en relation avec la fourniture de services de communications électroniques accessibles au public.

Art. 3. Sécurité du traitement

(1) Le fournisseur de services prend les mesures techniques et d'organisation appropriées afin de garantir la sécurité de ses services, le cas échéant conjointement avec l'opérateur en ce qui concerne la sécurité du réseau. En cas d'atteinte ou de risque d'atteinte grave à la sécurité du réseau ou des services, le fournisseur de services et le cas échéant l'opérateur prend les mesures appropriées pour y remédier, les frais étant à sa seule charge.

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 ~~de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel~~**, 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.

La Commission nationale pour la protection des données est habilitée à vérifier les mesures prises par les fournisseurs de services de communications électroniques accessibles au public, ainsi qu'à émettre des recommandations sur les meilleures pratiques concernant le degré de sécurité que ces mesures devraient atteindre.

(2) Sans préjudice de ce qui précède, le fournisseur de services et le cas échéant l'opérateur informe ses abonnés de tout risque imminent d'atteinte à la sécurité du réseau ou des services mettant en cause la confidentialité des communications ainsi que du moyen éventuel pour y remédier, y compris en en indiquant le coût probable.

(3) En cas de violation de données à caractère personnel, le fournisseur de services de communications électroniques accessibles au public avertit sans retard la Commission nationale pour la protection des données de la violation.

Lorsque la violation de données à caractère personnel est de nature à affecter négativement les données à caractère personnel ou la vie privée d'un abonné ou d'un particulier, le fournisseur avertit également sans retard indu l'abonné ou le particulier concerné de la violation.

La notification d'une violation des données à caractère personnel à l'abonné ou au particulier concerné n'est pas nécessaire si le fournisseur a prouvé, à la satisfaction de la Commission nationale pour la protection des données, qu'il a mis en œuvre les mesures de protection technologiques appropriées et que ces dernières ont été appliquées aux données concernées par ladite violation. De telles mesures de protection technologiques rendent les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès.

Sans préjudice de l'obligation du fournisseur d'informer l'abonné et le particulier concerné, si le fournisseur n'a pas déjà averti l'abonné ou le particulier de la violation de données à caractère personnel, la Commission nationale pour la protection des données peut, après avoir examiné les effets éventuellement négatifs de cette violation, exiger du fournisseur qu'il s'exécute.

La notification faite à l'abonné ou au particulier décrit au minimum la nature de la violation de données à caractère personnel et les points de contact auprès desquels des informations supplémentaires peuvent être obtenues et recommande des mesures à prendre pour atténuer les conséquences négatives possibles de la violation de données à caractère personnel. La notification faite à la Commission nationale pour la

protection des données décrit en outre les conséquences de la violation de données à caractère personnel, et les mesures proposées ou prises par le fournisseur pour y remédier.

La Commission nationale pour la protection des données peut adopter des lignes directrices et, le cas échéant, édicter des instructions précisant les circonstances dans lesquelles le fournisseur est tenu de notifier la violation de données à caractère personnel, le format applicable à cette notification et sa procédure de transmission.

Lors d'un premier manquement aux obligations de notification, le fournisseur est averti par la Commission nationale pour la protection des données. En cas de manquement répété la Commission nationale peut prononcer une amende d'ordre qui ne peut excéder 50.000 euros.

Un recours en réformation est ouvert devant le tribunal administratif contre les décisions prises par la Commission nationale pour la protection des données dans le cadre du présent article.

(4) Les fournisseurs tiennent à jour un inventaire des violations de données à caractère personnel, notamment de leur contexte, de leurs effets et des mesures prises pour y remédier, les données consignées devant être suffisantes pour permettre à la Commission nationale pour la protection des données de vérifier le respect des dispositions du paragraphe (3). Cet inventaire comporte uniquement les informations nécessaires à cette fin.

(5) Quiconque contrevient aux dispositions des paragraphes (1), (2) et (4) 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.

Art. 4. Confidentialité des communications

(1) Tout fournisseur de services ou opérateur garantit la confidentialité des communications effectuées au moyen d'un réseau de communications public et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes.

(2) Il est interdit à toute autre personne que l'utilisateur concerné d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance sans le consentement de l'utilisateur concerné.

(3) Le paragraphe (2):

(a) n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité;

(b) ne s'applique pas aux autorités judiciaires agissant dans le cadre des compétences leur attribuées par la loi et celles compétentes en vertu des articles 88-1 à 88-4 du Code d'instruction criminelle pour sauvegarder la sûreté de l'Etat, la défense, la sécurité publique et pour la prévention, la recherche, la constatation et la poursuite des infractions pénales ;

(c) ne s'applique pas aux communications et aux données relatives au trafic y afférentes, effectuées à destination du numéro d'appel d'urgence unique européen 112 et des numéros d'urgence déterminés par l'Institut dans le seul but de permettre (a) la réécoute de messages lors de

problèmes de compréhension ou d'ambiguïté entre l'appelant et l'appelé, (b) la documentation de fausses alertes, de menaces et d'appels abusifs et (c) la production de preuves lors de contestation sur le déroulement d'actions de secours.

Les données relatives au trafic afférentes aux communications visées ci-dessus, y compris les données de localisation, sont à effacer une fois le secours apporté. Le contenu des communications est à effacer après un délai de 6 mois au plus;

(d) n'affecte pas l'enregistrement de communications et des données relatives au trafic y afférentes, lorsqu'il est effectué dans le cadre des usages professionnels licites, afin de fournir la preuve d'une transaction commerciale ou de toute autre communication commerciale.

Les parties aux transactions ou à toutes autres communications commerciales sont informées au préalable de ce que des enregistrements sont susceptibles d'être effectués, de la ou des raisons pour lesquelles les communications sont enregistrées et de la durée de conservation maximale des enregistrements. Les communications enregistrées sont à effacer dès que la finalité est atteinte, et en tout état de cause, lors de l'expiration du délai légal de recours contre la transaction;

(e) ne s'applique pas au stockage d'informations, ou l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur à condition que l'abonné ou l'utilisateur ait donné son accord, après avoir reçu une information claire et complète, entre autres sur les finalités du traitement. Les méthodes retenues pour fournir l'information et offrir le droit de refus devraient être les plus conviviales possibles. Lorsque cela est techniquement possible et effectif, l'accord de l'abonné ou de l'utilisateur peut être exprimé par l'utilisation des paramètres appropriés d'un navigateur ou d'une autre application.

Cette disposition ne fait pas obstacle à un stockage ou à un accès techniques visant exclusivement à effectuer la transmission d'une communication par la voie d'un réseau de communications électroniques, ou strictement nécessaires au fournisseur pour la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur.

(4) 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.

Art. 5. Données relatives au trafic

~~**(1) (a)**~~ ~~***(Loi du 24 juillet 2010)***~~ **~~« 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, tout fournisseur de services ou opérateur qui traite ou génère dans le cadre de la fourniture de services des données relatives au trafic est tenu de conserver ces données pendant une période de six mois à compter 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. 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 ».~~

~~(b) Après la période de conservation prévue sub (a), le fournisseur de services ou l'opérateur est obligé d'effacer les données relatives au trafic concernant les abonnés et les utilisateurs, ou de les rendre anonymes.~~

~~(2)~~ **(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** ~~conservées pendant la période prévue sub (1) (a) de manière telle qu'il est impossible à quiconque d'accéder à ces données~~ 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** ~~sub (3) et (4)~~, 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 ~~et celles compétentes en vertu des articles 88-1 à 88-4 du Code d'instruction criminelle~~ pour sauvegarder **la sécurité nationale, pour la lutte contre la criminalité grave** ~~la sûreté de l'Etat, la défense,~~ **et pour la prévention de menaces graves contre** la sécurité publique ~~et pour la prévention, la recherche, la constatation et la poursuite des infractions pénales visées au paragraphe (1) (a)~~, ou

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

~~(3)~~ **(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.

~~(4)~~ **(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.

~~(5)~~ **(4)** Le traitement des données relatives au trafic effectué dans le cas des activités visées aux paragraphes **1er à 3** ~~(1) à (4)~~ 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.

(~~6~~) **(5)** Quiconque contrevient aux dispositions des paragraphes **1er à 4** ~~**(1) à (5)**~~ 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.

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.

Art. ~~5-1~~ 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** ~~**aux articles 22 et 23**~~ de ~~**la**~~ **cette même** loi ~~**modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.**~~

(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.

Art. ~~5-2.~~ 5*quater.* (1) La Commission nationale pour la protection des données ~~**transmet**~~ **publie** annuellement ~~**à la Commission de l'Union européenne**~~ 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.

Art. 6. Facturation détaillée

(1) Tout abonné a le droit de recevoir une facture non détaillée gratuite.

(2) Les appels gratuits y compris ceux aux lignes d'assistance ne sont pas indiqués sur la facture détaillée indépendamment de son degré de détail. En outre la facture détaillée ne contient aucune indication permettant d'identifier l'appelé.

Art. 7. Identification de la ligne appelante et de la ligne connectée

(1) Dans les cas où la présentation de l'identification de la ligne appelante est offerte, le fournisseur du service permet à l'abonné et à l'utilisateur appelant d'empêcher, par un moyen simple et gratuit, la présentation de l'identification de la ligne appelante et ce, appel par appel. L'abonné appelant dispose de cette possibilité de manière permanente pour chaque ligne.

(2) Dans les cas où la présentation de l'identification de la ligne appelante est offerte, l'abonné appelé doit pouvoir empêcher, par un moyen simple et gratuit pour un usage raisonnable de cette fonction, la présentation de l'identification de la ligne pour les appels entrants.

(3) Dans les cas où la présentation de l'identification de la ligne appelante est offerte et où l'identification de la ligne appelante est présentée avant l'établissement de l'appel, l'abonné appelé doit pouvoir, par un moyen simple et gratuit, refuser les appels entrants lorsque l'utilisateur ou l'abonné appelant a empêché la présentation de l'identification de la ligne appelante.

(4) Dans le cas où la présentation de l'identification de la ligne connectée est offerte, l'abonné appelé doit pouvoir, par un moyen simple et gratuit, empêcher la présentation de l'identification de la ligne connectée à l'utilisateur appelant.

(5) (a) Tout fournisseur ou opérateur de services de téléphonie fixe ou mobile qui fournit un accès au numéro d'appel d'urgence unique européen 112 ainsi qu'aux numéros d'urgence déterminés par l'Institut luxembourgeois de régulation transmet (« push ») pour chaque appel à destination d'un de ces numéros d'appel d'urgence les données disponibles concernant l'appelant y compris les données de localisation.

Aux termes du présent paragraphe on entend par « données disponibles »:

– les données relatives à l'identification: le numéro de téléphone, nom, prénom(s), domicile ou lieu de résidence habituel, dénomination ou raison sociale, lieu d'établissement de l'abonné et de l'utilisateur pour autant que ce dernier soit identifié ou identifiable; l'indication du caractère public ou non public des données, ainsi que

– toutes les données traitées dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public (données de localisation).

(b) L'Institut luxembourgeois de régulation fixe, en cas de besoin, le format et les modalités techniques de mise à disposition des données visées au paragraphe (5) et au paragraphe (5*bis*).

(c) Pour les appels effectués à destination du numéro d'appel d'urgence unique européen 112 et des numéros d'urgence déterminés par l'Institut, l'identification de la ligne appelante et les données de localisation de l'appelant » est toujours présentée même lorsque l'appelant l'a empêchée.

(5*bis*) En outre, en cas **~~d'appel~~ 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 ~~au~~** numéro d'urgence unique européen 112 ainsi **que vers les ~~qu'aux~~** 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.

(6) Les dispositions du paragraphe (1) s'appliquent également aux appels provenant de l'Union européenne à destination de pays tiers. Les dispositions des paragraphes (2), (3) et (4) s'appliquent également aux appels entrants provenant de pays tiers.

(7) Le fournisseur du service informe le public, par des moyens appropriés et au plus tard lors de la conclusion d'un contrat des possibilités sus énoncées.

(8) L'abonné appelé prétendant être victime d'appels à contenu malveillant ou dérangeant peut demander l'identification de la ligne appelante ou connectée, des appels répétés ou intempestifs, déclarés comme étant malveillants ou dérangeants, lesquels ont été effectués ou repérés sur base d'un même numéro d'appel ou d'un même raccordement. Un règlement grand-ducal fixera les modalités à respecter par le fournisseur du service ou l'opérateur ainsi que par les abonnés prétendant être victime d'appels à contenu malveillant ou dérangeant. Il précisera également les caractéristiques d'un appel à contenu malveillant ou dérangeant et déterminera l'utilisation de l'identification de la ligne appelante même si sa présentation est empêchée.

(9) 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.

Art. 8. Renvoi automatique d'appels

Dans le cas où le renvoi automatique d'appels (ou déviation) est offert, le fournisseur du service confère à tout abonné la possibilité de mettre fin, par un moyen simple et gratuit, au renvoi automatique d'appels par un tiers vers son appareil terminal lorsque le fournisseur du service peut identifier l'origine des appels renvoyés. Le cas échéant, cette identification se fait en collaboration avec d'autres fournisseurs de services concernés.

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

~~(1) (a)~~ ~~*(Loi du 24 juillet 2010)* « 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, tout fournisseur de services ou opérateur qui traite ou génère dans le cadre de la fourniture de services des données de localisation autres que des données relatives au trafic est tenu de conserver ces données pendant une période de six mois à compter 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 de localisation autres que les 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 ».~~

~~(b) Après la période de conservation prévue sub (a), le fournisseur de services ou l'opérateur est obligé d'effacer les données de localisation autres que les données relatives au trafic concernant les abonnés et les utilisateurs, ou de les rendre anonymes.~~

~~(2)~~ **(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,** ~~conservées pendant la période prévue au paragraphe (1), (a) de manière telle qu'il est impossible à quiconque d'accéder à ces données~~, 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 ~~et celles compétentes en vertu des articles 88-1 à 88-4 du Code d'instruction criminelle~~ pour sauvegarder **la sécurité nationale, pour la lutte contre la criminalité grave** ~~la sûreté de l'Etat, la défense,~~ **et pour la prévention de menaces graves contre** la sécurité publique ~~et pour la prévention, la recherche, la constatation et la poursuite des infractions pénales visées au paragraphe (1) (a)~~.

~~(3)~~ **(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** ~~**(2), (4) et (5)**~~.

~~**(4)**~~ **(3)** Le fournisseur ~~**du service**~~ **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.

~~**(5)**~~ **(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** ~~**(1) à (4)**~~ 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.

~~**(6)**~~ **(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.

*

[articles 10 et 10bis inchangés]

*

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.

*

[article 11 inchangé]

*

Art. 12. Commission nationale pour la protection des données

La Commission nationale pour la protection des données instituée par l'article ~~**32 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel**~~ **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 ~~**8 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel**~~ **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**.

*

[articles 12bis à 16 inchangés]

*

3. Loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat

Art. 7. – ***Moyens et mesures de recherche soumis à l'autorisation du Comité après l'assentiment de la commission spéciale***

(1) [écoutes]

(2) Sous réserve de respecter les principes de proportionnalité et de subsidiarité, le SRE est autorisé à procéder au repérage 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, en requérant au besoin le concours technique de l'opérateur de télécommunications et/ou du fournisseur d'un service de ~~**télécommunications**~~ **communications électroniques.**

La durée de cette mesure de recherche ne pourra se reporter qu'à une période maximale de six mois précédant ou suivant la date à laquelle elle a été ordonnée, sans préjudice de renouvellement.

Toute personne qui, du chef de sa fonction, a connaissance d'une des mesures prises en exécution du présent article 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.

Lorsque les mesures de repérage de télécommunications ne donnent aucun résultat, les données obtenues sont détruites immédiatement par le SRE. Lorsque les renseignements obtenus peuvent servir à la continuation de l'enquête, la destruction a lieu au plus tard cinq ans après la clôture de l'enquête et lorsque les faits faisant l'objet de l'enquête ont été dénoncés au procureur, la destruction a lieu au plus tard au moment de la prescription de l'action publique.

(3) Les décisions de surveillance et de contrôle visées au paragraphe 1er ainsi que les décisions de repérage visées au paragraphe 2 sont notifiées aux opérateurs des services concernés qui font procéder sans retard à leur exécution.

Lorsque les mesures de surveillance et de contrôle visées au paragraphe 1er n'ont donné aucun résultat, les copies, enregistrements, données et renseignements obtenus sont immédiatement détruits par le SRE.

Au cas où ces copies, enregistrements, données et renseignements, peuvent servir à la continuation de l'enquête la destruction a lieu au plus tard cinq ans après la clôture de l'enquête et lorsque les faits faisant l'objet de l'enquête ont été dénoncés au procureur, la destruction a lieu au plus tard au moment de la prescription de l'action publique.

Les correspondances sont mises sous scellés et remises contre récépissé au SRE, qui fait copier les correspondances pouvant servir à ses investigations et renvoie les écrits qu'il ne juge pas nécessaire de retenir aux opérateurs qui les font remettre au destinataire.

Les communications avec des personnes liées par le secret professionnel au sens de l'article 458 du Code pénal et non suspectes elles-mêmes d'être impliquées dans une menace actuelle ou potentielle relevant du champ d'application sont immédiatement détruits par le SRE.

(4) Les mesures de surveillance et de contrôle visées au paragraphe 1er ainsi que les mesures de repérage visées au paragraphe 2 sont ordonnées par le Comité sur demande écrite du directeur du SRE et après l'assentiment d'une commission composée par le président de la Cour supérieure de justice, le président de la Cour administrative et le président du tribunal d'arrondissement de Luxembourg, désignée ci-après « la commission spéciale ».

En cas d'empêchement le président de la Cour supérieure de justice est remplacé par un vice-président, le président de la Cour administrative par un vice-président et le président du tribunal d'arrondissement par le premier vice-président le plus ancien en rang.

En cas d'urgence le ministre peut de sa propre autorité ordonner les mesures de surveillance et de contrôle visées au paragraphe 1er ainsi que les mesures de repérage visées au paragraphe 2, sauf à saisir sans désemparer le Comité et la commission spéciale. Toute décision relative au renouvellement d'une opération de repérage, de surveillance et du contrôle intervient dans les conditions de l'alinéa 1.

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 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. 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.

___