

N° 8148

CHAMBRE DES DEPUTES

Session ordinaire 2022-2023

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 élec-
troniques ; et**
- 3° de la loi modifiée du 5 juillet 2016 portant réorganisation
du Service de renseignement de l'Etat**

* * *

Document de dépôt

Dépôt: le 8.2.2023

*

ARRETE GRAND-DUCAL DE DEPOT

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

Sur le rapport de Notre Ministre de la Justice et après délibération du Gouvernement en Conseil ;

Arrêtons :

Article unique. – Notre Ministre de la Justice est autorisée à déposer en Notre nom à la Chambre des Députés le 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.

Palais de Luxembourg, le 3 février 2023

La Ministre de la Justice,
Sam TANSON

HENRI

*

TEXTE DU PROJET DE LOI

Art. 1^{er}. 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 1^{er}, 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 1^{er} 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 1^{er} 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'État.

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 1^{er} 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 1^{er}, 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 1^{er} 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 1^{er} 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 *5bis* nouveau, libellé comme suit :

« Art. 5bis. (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 événements 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 1^{er} 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 *5ter* nouveau, est remplacé comme suit :

« Art. *5ter*. (1) Les données conservées au titre des articles 5, *5bis* et 9 de la présente loi par les autorités compétentes au sens de l'article 1^{er}, paragraphe 1^{er}, de la loi du 1^{er} 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 *5quater* nouveau, est remplacé comme suit :

« Art. *5quater*. (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 *5bis*, de la même loi est modifié comme suit :

« (*5bis*) 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 1^{er}, 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 1^{er} 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 1^{er} 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 1^{er} 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 1^{er} 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 1^{er} 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 1^{er}, 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 1^{er} 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 1^{er}, l'article 2, points 3^o, 4^o et 7^o, 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.

*

EXPOSE DES MOTIFS

Le présent projet de loi a pour objet d'adapter le dispositif légal national relatif à la rétention des données dans le secteur des communications électroniques aux exigences des derniers arrêts rendus par la Cour de Justice de l'Union européenne dans la matière, et notamment l'arrêt « Quadrature du Net » du 6 octobre 2020 (affaires C-511/18, C-512/18 et C-520/18 : La Quadrature du Net, French Data Network et Ordre des barreaux francophones et germanophone) ainsi que l'arrêt dans l'affaire C-140/20 « Commissioner of the Garda Síochána e.a. » du 5 avril 2022.

*

1. CONTEXTE JURIDIQUE

a) Cadre juridique européen

La **directive 95/46/CE** du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données oblige les États membres à assurer la protection des libertés et des droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel, afin d'assurer la libre circulation de ces données dans la Communauté.

La **directive 2002/58/CE** du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) traduit les principes définis dans la directive 95/46/CE en règles spécifiques au secteur des communications électroniques.

Les articles 5, 6 et 9 de la directive 2002/58/CE définissent les règles applicables au traitement, par les fournisseurs de réseaux et de services, de données relatives au trafic et de données de localisation générées par l'utilisation de services de communications électroniques. Ces données doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication, sauf les données requises pour établir les factures et les paiements pour interconnexion; moyennant l'accord de l'intéressé, certaines données peuvent également être traitées à des fins commerciales ou de fourniture de services à valeur ajoutée.

L'article 15, paragraphe 1^{er}, de la directive 2002/58/CE énumère les conditions dans lesquelles les États membres peuvent limiter la portée des droits et des obligations à ladite directive. Toute limitation de ce type doit constituer une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour des raisons spécifiques d'ordre public, à savoir pour sauvegarder la sécurité nationale, la défense et la sécurité publique, ou pour assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées de systèmes de communications électroniques.

Suite aux attentats terroristes perpétrés à Madrid le 11 mars 2004 et à Londres le 7 juillet 2005, la **directive 2006/24/CE** sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques voit le jour, établissant un socle commun européen relatif à la conservation obligatoire, par les opérateurs, des données de trafic et de localisation, ainsi que les données y relatives, pour les besoins des autorités.

L'objectif principal de la Directive 2006/24/CE était d'obliger les opérateurs et fournisseurs de services de communications électroniques accessibles au public ou de réseaux de communications

publics à conserver ces données de trafic et de localisation pour une période d'au moins six mois. La conservation de ces données était considérée comme étant nécessaire à l'identification des abonnés ou des utilisateurs et avait pour objectif d'assurer la disponibilité des données à des fins de prévention, d'enquêtes, de détection et de poursuites des infractions pénales, telles que le crime organisé et le terrorisme.

b) Cadre juridique national

L'obligation de conservation des données de trafic et de localisation relatives aux communications électroniques a été introduite dans la législation luxembourgeoise par la **loi du 30 mai 2005** concernant la protection de la vie privée dans le secteur des communications (dénommée ci-après la « Loi Telecom ») sur base de l'article 15, paragraphe 1^{er} de la directive 2002/58/CE.

Puis, la **loi du 27 juillet 2007** portant modification de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel; des articles 4 paragraphe (3) lettre d); 5 paragraphe (1) lettre a); 9 paragraphe (1) lettre a) et 12 de la Loi Telecom et de l'article 23 paragraphe (2) points 1. et 2. de la loi du 8 juin 2004 sur la liberté d'expression dans les médias a ramené à six mois le délai de conservation initialement fixé à douze mois.

La directive 2006/24/CE a été transposée au Luxembourg par les dispositions de la **loi du 24 juillet 2010** portant modification des articles 5 et 9 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et de l'article 67-1 du Code d'instruction criminelle, assorties par ailleurs d'un règlement grand-ducal du même jour qui en a réglé les modalités d'application.

Les opérateurs nationaux sont donc tenus à conserver les données de trafic et de localisation au sens des articles 5 et 9 de la Loi Telecom et l'accès à ces données est garanti au juge d'instruction moyennant l'article 67-1 du Code de procédure pénale et au Service de renseignement de l'Etat au sens de l'article 7 de la loi modifiée du 5 juillet 2016 portant réorganisation du SRE.

*

2. EVOLUTION DE LA JURISPRUDENCE EUROPEENNE

a) L'arrêt fondamental : « *Digital Rights Ireland* » du 8 avril 2014¹

Le 8 avril 2014, dans l'arrêt « *Digital Rights Ireland* », la CJUE a déclaré la Directive 2006/24/EC invalide, au motif que l'ingérence que comporte l'obligation générale de conservation des données relatives au trafic et des données de localisation imposée par celle-ci dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel n'était pas limitée au strict nécessaire.

Les points essentiels de l'arrêt concernant l'encadrement manquant peuvent se résumer comme suit :

- **Limitations quant à la conservation :**

La directive prévoyait une conservation généralisée et indifférenciée, aucune distinction n'étant faite en fonction de l'existence ou non d'un lien, même indirect ou lointain, avec une infraction, et aucune exception n'étant applicable aux personnes soumises au secret professionnel ;

- **Limitations quant à l'accès et l'utilisation ultérieure :**

La directive ne prévoyait aucun critère objectif permettant de restreindre ces traitements à des fins de prévention, de détection ou de poursuites pénales d'infractions d'un niveau de gravité suffisant, ni les conditions matérielles et procédurales y afférentes ;

- **Limitations quant à la durée de conservation des données :**

La période prévue était de minimum six mois et de maximum vingt-quatre mois, sans distinction entre les catégories de données selon leur utilité et sans prévoir la nécessité de critères objectifs garantissant que cette durée soit limitée au strict nécessaire ;

¹ CJUE, 8 avril 2014, *Digital Rights Ireland* et *Seitlinger*, affaires jointes C293/12 et C594/12.

- **Garanties en termes de sécurité et de protection des données conservées :**

La directive n'incluait pas de mesures adéquates visant à garantir leur intégrité et leur confidentialité, ainsi que leur conservation sur le territoire de l'Union de manière à assurer un contrôle effectif par une autorité indépendante

b) L'arrêt de consécration : « Tele2 et Watson » du 21 décembre 2016²

L'arrêt de la CJUE rendu le 21 décembre 2016 confirme et consacre sa lecture stricte de l'interdiction de la conservation généralisée et indifférenciée.

Néanmoins, si la Cour condamne les législations nationales comme excédant les limites du strict nécessaire, elle laisse la porte ouverte à « *une réglementation permettant, à titre préventif, la conservation ciblée des données relatives au trafic et des données de localisation, à des fins de lutte contre la criminalité grave, à condition que la conservation des données soit, en ce qui concerne les catégories de données à conserver, les moyens de communication visés, les personnes concernées ainsi que la durée de conservation retenue, limitée au strict nécessaire* »³.

c) L'arrêt d'atténuation : « Quadrature du Net et FDN » et « Privacy International » du 6 octobre 2020⁴

Par l'arrêt La Quadrature du Net du 6 octobre 2020 concernant trois affaires jointes⁵ dans le cadre de recours en annulation portés à l'encontre de mesures de droit national, la CJUE maintient l'interdiction de principe de l'obligation de conservation généralisée et indifférenciée des données de connexion, toujours sur la base des mêmes arguments. Néanmoins, elle tempère sa condamnation de la conservation généralisée et indifférenciée des données de communications électroniques et y apporte des précisions.

Tout d'abord, la CJUE souligne que le principe de garantie de confidentialité des communications et des données y afférentes peut être battu en brèche, dès lors qu'une limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale, la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales. Une « pondération équilibrée » doit être ainsi réalisée entre ces derniers et les droits fondamentaux en cause.

S'agissant des mesures législatives prévoyant la **conservation préventive des données relatives au trafic et des données de localisation aux fins de la sauvegarde de la sécurité nationale**, la Cour n'énonce pas de prime abord une interdiction de toute conservation généralisée et indifférenciée desdites données. Bien au contraire, la Cour souligne le caractère supérieur de l'objectif de sauvegarde de la sécurité nationale, estimant que ce dernier est « *susceptible de justifier des mesures comportant des ingérences dans les droits fondamentaux plus graves que celles que pourraient justifier [l]es autres objectifs* »⁶. La conservation généralisée et indifférenciée des données de trafic et de localisation (autres que les données d'identité civile et les adresses IP à la source de la connexion) peut donc être imposée aux opérateurs en cas de menace grave, réelle et actuelle ou prévisible pour la sécurité nationale.

S'agissant, ensuite, des mesures législatives prévoyant la **conservation préventive des données relatives au trafic et des données de localisation aux fins de la lutte contre la criminalité et de la sauvegarde de la sécurité publique**, la CJUE, suivant en cela ses jurisprudences précédentes, estime que seule la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique sont de nature à justifier des ingérences graves dans les droits fondamentaux. Soulignant ici le caractère sensible des informations concernées, la Cour voit dans leur conservation une ingérence grave, concernant la quasi-totalité de la population, sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif poursuivi.

² CJUE, 21 décembre 2016, Tele2 Sverige AB (C-203/15) et Secretary of State for the Home Department, affaire C-698/15.

³ Paragraphe 108 de l'arrêt de 2016.

⁴ CJUE, 6 octobre 2020, Privacy international (affaire C-623/17), et La Quadrature du Net, French Data Network, Ordre des barreaux francophones et germanophone (affaires jointes C-511/18, C-512/18, C-520-18).

⁵ Les arrêts de la Cour de justice répondent à des questions préjudicielles soulevées respectivement par le tribunal britannique chargé des pouvoirs d'enquête, par le Conseil d'État français et par la Cour constitutionnelle belge.

⁶ Paragraphe 136 de l'arrêt de 2020.

La Cour ne ferme pas pour autant toutes les portes, puisqu'elle souligne néanmoins qu'une **conservation ciblée** (ciblant des catégories de personnes ou des lieux) de données relatives au trafic et de données de localisation est possible, afin de répondre aux objectifs de lutte contre la criminalité grave et de prévention d'atteintes graves à la sécurité publique.

La CJUE souligne également que des **exceptions au principe d'interdiction** de tout stockage de masse de façon généralisée et indifférenciée sont possibles. Elle permet ainsi des mesures législatives prévoyant:

- la **conservation préventive généralisée et indifférenciée des adresses IP** aux fins de la lutte contre la criminalité et de la sauvegarde de la sécurité publique.

Selon la Cour, les données d'adresses IP, permettant d'identifier la personne physique propriétaire de l'équipement terminal à partir duquel une communication au moyen de l'Internet est effectuée, présentent un « *degré de sensibilité moindre que les autres données relatives au trafic* », même si elles peuvent permettre le « *traçage exhaustif du parcours de navigation d'un internaute* » concourant à « *établir le profil détaillé de ce dernier* »⁷. Pour la Cour, une mesure législative prévoyant la conservation généralisée et indifférenciée des seules adresses IP n'apparaît pas, en principe, contraire à l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, pourvu que cette possibilité soit soumise au strict respect des conditions matérielles et procédurales devant régir l'utilisation de ces données. La Cour souligne toutefois que seule la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique sont de nature, à l'instar de la sauvegarde de la sécurité nationale, à justifier cette ingérence.

- la **conservation préventive généralisée et indifférenciée des données relatives à l'identité civile** aux fins de la lutte contre la criminalité et de la sauvegarde de la sécurité publique.

La CJUE estime que l'ingérence que comporte une conservation de ces données ne saurait, en principe, être qualifiée de grave. Elle en conclut dès lors que des « *mesures législatives visant le traitement de ces données en tant que telles, notamment leur conservation et l'accès à celles-ci à la seule fin de l'identification de l'utilisateur concerné, et sans que lesdites données puissent être associées à des informations relatives aux communications effectuées, sont susceptibles d'être justifiées par l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général* »⁸.

- la **conservation rapide des données relatives au trafic et des données de localisation** aux fins de la lutte contre la criminalité grave.

Il s'agit ici de conserver les données en question au-delà du délai légal normalement prévu, aux fins de l'élucidation d'infractions pénales graves ou d'atteintes à la sécurité nationale, « *et ce tant dans la situation où ces infractions ou ces atteintes ont déjà pu être constatées que dans celle où leur existence peut, au terme d'un examen objectif de l'ensemble des circonstances pertinentes, être raisonnablement soupçonnée* »⁹. La Cour va reconnaître encore aux autorités nationales la « *possibilité, au moyen d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, d'enjoindre aux fournisseurs de services de communications électroniques de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont ils disposent* »¹⁰. La Cour insiste toutefois sur l'encadrement étroit des modalités d'une telle conservation, qui doit être limitée au strict nécessaire, s'agissant notamment de la durée de conservation. La finalité d'une telle conservation doit en outre être clairement établie et enfin, et surtout, seule la lutte contre la criminalité grave et, a fortiori, la sauvegarde de la sécurité nationale, sont de nature à justifier une telle ingérence.

⁷ Paragraphes 152 et 153 de l'arrêt de 2020.

⁸ Paragraphes 157 et 158 de l'arrêt de 2020.

⁹ Paragraphe 161 de l'arrêt de 2020.

¹⁰ Paragraphe 163 de l'arrêt de 2020.

d) L'arrêt de précision : « Commissioner of the Garda Síochána e.a » du 5 avril 2022¹¹

La grande chambre de la CJUE, dans une décision du 5 avril 2022, confirme sa jurisprudence récente selon laquelle le droit de l'UE s'oppose à une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation afférentes aux communications électroniques afin de lutter contre les infractions graves.

Mais, elle apporte en outre de nouvelles précisions sur les conditions dans lesquelles des dérogations à cette règle, strictement encadrées et conformes au principe de proportionnalité, sont possibles. Elle offre ainsi une trame pour un dispositif dérogatoire compatible avec le droit de l'UE et apporte des précisions sur les catégories de mesures envisageables.

- Une **conservation ciblée** des données relatives au trafic et à la localisation en fonction de **catégories de personnes concernées ou au moyen d'un critère géographique**

Les autorités nationales peuvent prendre une mesure de conservation fondée sur un critère géographique comme le taux moyen de criminalité dans une zone géographique donnée, sans qu'elles disposent nécessairement d'indices concrets portant sur la préparation ou la commission, dans les zones concernées, d'actes de criminalité grave.

Une telle mesure de conservation, qui vise des lieux ou des infrastructures fréquentées régulièrement par un nombre très élevé de personnes ou des lieux stratégiques (aéroports, gares, ports maritimes, zones de péage) est susceptible de permettre aux autorités :

- d'obtenir des informations sur la présence, dans ces lieux, des personnes qui y utilisent un moyen de communication électronique ;
- d'en tirer les conclusions sur leur présence et leurs activités dans ces lieux afin de lutter contre la criminalité grave.

- Une **conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion**

La directive ne s'oppose pas non plus à des mesures législatives qui prévoient, aux mêmes fins, une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire.

- Une **conservation généralisée et indifférenciée des données relatives à l'identité civile** des utilisateurs de moyens de communications électroniques

Ni la directive e-privacy ni aucun autre acte de l'Union ne s'opposent à une législation nationale qui a pour objet la lutte contre la criminalité grave et qui subordonne l'acquisition d'un moyen de communication électronique (carte SIM prépayée par exemple) à la vérification de documents d'identité officiels et à l'enregistrement, par le vendeur, des informations qui en résultent. Le vendeur étant, le cas échéant, tenu de donner accès à ces informations aux autorités nationales compétentes.

- Une **conservation rapide (*quick freeze*)** des données relatives au trafic et à la localisation dont disposent ces fournisseurs de services

La Cour juge que les autorités compétentes peuvent ordonner une mesure de conservation rapide dès le premier stade de l'enquête portant sur une menace grave pour la sécurité publique ou sur un éventuel acte de criminalité grave. Une telle mesure, précise la Cour, peut être étendue aux données relatives au trafic et à la localisation afférentes à des personnes autres que celles qui sont soupçonnées d'avoir projeté ou commis une infraction pénale grave ou une atteinte à la sécurité nationale. À la condition cependant que ces données puissent, sur la base d'éléments objectifs et non discriminatoires, contribuer à l'élucidation d'une telle infraction (données de la victime, données de l'entourage social ou professionnel).

Cependant, précise la Cour, toutes ces mesures doivent assurer, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus.

¹¹ CJUE, 5 avril 2022, G.D. contre Commissioner of An Garda Síochána, affaire C-140/20.

Ces différentes mesures peuvent, selon le choix du législateur national et tout en respectant les limites du strict nécessaire, trouver à s'appliquer conjointement.

**e) Les arrêts de confirmation : «SpaceNet » et « VD »
du 20 septembre 2022¹²**

Dans les deux affaires jointes C-793/19 et C-794/19 « SpaceNet », deux demandes de décision préjudicielle ont été présentées par le Bundesverwaltungsgericht (Cour administrative fédérale allemande), qui a été saisi d'un recours en « Revision » par la République fédérale d'Allemagne contre deux arrêts ayant accueilli les recours formés par deux sociétés, SpaceNet AG et Telekom Deutschland GmbH, fournissant des services d'accès à Internet. Par ces recours, ces sociétés contestaient l'obligation qu'impose la réglementation allemande de conserver des données relatives au trafic et des données de localisation afférentes aux communications électroniques de leurs clients. Par son arrêt, la CJUE confirme la jurisprudence issue des arrêts du 6 octobre 2020 et du 5 avril 2022. Elle rappelle notamment que la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation afférentes aux communications électroniques n'est pas autorisée, à titre préventif, aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique. En revanche, conformément aux jurisprudences précédentes, la CJUE ne s'oppose pas à une législation nationale qui prévoit les types de conservations généralisées ou ciblées détaillées par l'arrêt du 5 avril 2022.

Puis, concernant l'affaire de la CJUE du même jour C-339/20 « VD », des procédures pénales ont été engagées en France contre VD et SR des chefs de délits d'initiés, de recel de délits d'initiés, de complicité, de corruption et de blanchiment. Ces procédures avaient pour origine des données à caractère personnel issues d'appels téléphoniques effectués par VD et SR, générées dans le cadre de la fourniture de services de communications électroniques, qui avaient été communiqués au juge d'instruction par l'Autorité des marchés financiers à la suite d'une enquête diligentée par cette dernière. La CJUE confirme dans le même sens sa jurisprudence selon laquelle le droit de l'Union s'oppose à ce qu'une juridiction nationale limite dans le temps les effets d'une déclaration d'invalidité qui lui incombe, en vertu du droit national, à l'égard d'une législation nationale imposant aux fournisseurs de services de communications électroniques une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, en raison de l'incompatibilité de cette législation avec la directive « vie privée et communications électroniques ».

*

3. ANTECEDANTS NATIONAUX

La directive 2006/24/CE a été invalidée compte tenu de la portée de l'ingérence dans l'exercice des droits fondamentaux que comporte l'obligation faite aux fournisseurs de services de communications électroniques de conserver les données de trafic et de localisation des utilisateurs ainsi que de l'absence de proportionnalité et de règles claires et suffisantes imposant des limites et mesures de sauvegarde.

Il convient partant de noter que la CJUE s'est prononcé contre l'obligation de la rétention des données dans les conditions de la directive 2006/24/CE, sans pour autant invalider le principe même d'une conservation de données.

Cependant, puisque la directive 2006/24/CE est déclarée invalide, le retour au statu quo ante s'impose : les ordres juridiques de l'Union et de ses Etats membres en reviennent à la situation antérieure à l'entrée en vigueur de la directive, donc à la situation existante au 31 décembre 2005. Les Etats membres n'ont plus l'obligation mais simplement la possibilité de demander aux opérateurs de téléphonie et aux fournisseurs d'accès de conserver les données de télécommunication électroniques aux fins de recherche, détection et poursuite d'infractions pénales.

Afin de répondre aux problèmes soulevés par la CJUE dans son Arrêt « *Digital Rights Ireland* », le projet de loi n° 6763 portant modification du Code d'instruction criminelle et de la loi modifiée du

¹² CJUE, 20 septembre 2022, SpaceNet, affaires jointes C-793/19 et C-794/19 ;

CJUE, 20 septembre 2022, VD, affaires jointes C-339/20 et C-397/20.

30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques a été déposé à la Chambre des Députés en date du 7 janvier 2015.

Ledit projet de loi avait comme objectif d'adapter le dispositif légal relatif à la rétention des données à des fins de poursuites pénales aux exigences de la jurisprudence européenne. Le texte tel que proposé a certes introduit une obligation de destruction irrémédiable des données retenues après l'expiration du délai de rétention, mais le principe de la conservation généralisée et indifférenciée des données pendant une durée de six mois est néanmoins maintenu.

Etant donné que ledit projet de loi ne correspond donc plus aux critères énoncés par la CJUE dans ses différents arrêts, un nouveau texte a été élaboré en visant à garantir l'équilibre entre, l'accès aux données traitées par des fournisseurs de communications électroniques dans le cadre de la lutte contre le terrorisme et la criminalité grave, d'une part, et la protection de la vie privée des citoyens, d'autre part.

*

4. FINALITE DE LA RETENTION DES DONNES

À l'exclusion du contenu de la communication en tant que tel, les données concernées sont celles nécessaires pour retrouver et identifier la source d'une communication et la destination de celle-ci, pour déterminer la date, l'heure, la durée et le type d'une communication, le matériel de communication des utilisateurs, ainsi que pour localiser le matériel de communication mobile, données au nombre desquelles figurent, notamment, le nom et l'adresse de l'abonné ou de l'utilisateur inscrit, le numéro de téléphone de l'appelant et le numéro appelé ainsi qu'une adresse IP pour les services Internet.

La rétention de ces données de trafic et de localisation permet notamment de savoir quelle est la personne avec laquelle un utilisateur a communiqué et par quel moyen, tout comme de déterminer le temps de la communication ainsi que l'endroit à partir duquel celle-ci a eu lieu. En outre, elles permettent de connaître la fréquence des communications de l'utilisateur avec certaines personnes pendant une période donnée.

Ces données sont utiles au niveau de la réalisation de la politique criminelle. Elles permettent, notamment, d'établir dans le cadre de crimes violents, quel individu était actif autour des scènes de crimes, de pouvoir localiser le téléphone portable utilisé et le moment de son utilisation ou encore d'identifier un téléphone portable utilisé au moment des faits. De la même manière, dans le cadre de recherches liées à un réseau d'auteurs, les enquêteurs peuvent déterminer sur la base des données conservées, quelle personne a été en contact avec qui et où se trouvent les éventuels lieux de rencontre.

Dans le cadre de la prévention d'actes terroristes, la conservation des données de trafic et de localisation permet aux services de renseignement de réaliser une analyse rétrospective des communications d'une personne suspectée de préparer un attentat, permettant ainsi de déjouer cette tentative et d'identifier de potentiels réseaux. Il en est de même pour l'ensemble des menaces, croissantes, affectant la sécurité nationale, qu'il s'agisse d'ingérence étrangère, de cyberattaques, de criminalité organisée ou d'atteinte aux intérêts économiques et sociaux fondamentaux.

Les repérages téléphoniques sont d'ailleurs utilisés à charge et à décharge de la personne suspectée et peuvent servir à confirmer l'alibi d'une personne. L'accès aux données de connexion permet ainsi d'innocenter des suspects et de protéger d'éventuelles victimes, par exemple, en cas d'enlèvement.

Eu égard néanmoins le constat qu'une conservation généralisée et indifférenciée des données relatives au trafic ou à la localisation constitue une ingérence dans les droits fondamentaux, alors qu'elle dépasse le strict nécessaire, le présent projet de loi vise à limiter cette conservation.

*

5. SOLUTIONS PROPOSEES DANS LE CADRE DES POSSIBILITES LAISSEES PAR LA JURISPRUDENCE EUROPEENNE

En premier lieu, le présent projet de loi propose dès lors la suppression du principe de conservation généralisée et indifférenciée des données relatives au trafic et à la localisation, tel que prévu aux articles 5 et 9 de la Loi Telecom (article 2 du projet de loi).

Puis, le présent projet de loi propose, conformément à la jurisprudence européenne la conservation généralisée et indifférenciée :

- des données d'identification et des adresses IP attribuées à la source de connexion aux fins de la lutte contre la criminalité grave et de la sauvegarde de la sécurité publique (article 2, point 9° du projet de loi) ; et
- des données relatives au trafic et des données de localisation aux seules fins de la sauvegarde de la sécurité nationale (article 3, point 2° du projet de loi).

En outre, le projet de loi suggère la création de mesures législatives permettant la conservation ciblée de données, et notamment :

- la conservation ciblée des données relatives au trafic et à la localisation en fonction de catégories de personnes concernées ou au moyen d'un critère géographique (article 2, point 4° du projet de loi) ;
- la conservation rapide des données relatives au trafic et à la localisation dont disposent les opérateurs ou fournisseurs de services concernés (article 1^{er}, point 1° du projet de loi concernant la lutte contre la criminalité grave et de la sauvegarde de la sécurité publique et article 3, point 3° du projet de loi concernant la sauvegarde de la sécurité nationale).

*

Le projet de loi sous rubrique entend dès lors répondre aux exigences de la jurisprudence européenne en permettant une conciliation entre les deux exigences que sont sécurité et liberté.

L'enjeu du texte proposé est d'encadrer la conservation et l'usage des données de trafic et de localisation sans priver ces données de leur valeur utile, notamment en fixant des conditions strictes d'accès et de durée de conservation.

Le Gouvernement considère que ledit projet de loi permet une pondération équilibrée entre l'objectif d'intérêt général et les droits en cause, tout en garantissant que l'importance de cet objectif est en relation avec la gravité de l'ingérence que comporte la conservation des données de communication.

*

COMMENTAIRE DES ARTICLES

Article 1^{er} du projet de loi – modifications du Code de procédure pénale :

Ad Point 1° – article 24-3 du Code de procédure pénale :

Dans ses arrêts du 6 octobre 2020¹ et du 5 avril 2022², la Cour de justice de l'Union européenne (dénommée ci-après la « CJUE ») a jugé de manière générale que « *en ce qui concerne l'objectif de lutte contre la criminalité grave, (...) une législation nationale prévoyant, à cette fin, la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation excède les limites du strict nécessaire et ne saurait être considérée comme étant justifiée dans une société démocratique* ».

Cependant, l'arrêt du 6 octobre 2020 permet des mesures législatives permettant le recours à une conservation ciblée, temporellement limitée au strict nécessaire, des données relatives au trafic et à la localisation, qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées³. La Cour précise ainsi que la mesure de conservation peut « *viser les personnes dont les données relatives au trafic et les données de localisation sont susceptibles de révéler un lien, au moins indirect, avec des actes de criminalité grave, de contribuer d'une manière ou d'une autre à la lutte contre la criminalité grave ou de prévenir un risque grave pour la sécurité publique (...)* »⁴.

1 CJUE, 6 octobre 2020, Privacy international (affaire C-623/17), et La Quadrature du Net, French Data Network, Ordre des barreaux francophones et germanophone (affaires jointes C-511/18, C-512/18, C-520-18).

2 CJUE, 5 avril 2022, G.D. contre Commissioner of An Garda Síochána, affaire C-140/20.

3 Paragraphes 140 et suivants de l'arrêt du 6 octobre 2020.

4 Paragraphe 148 de l'arrêt du 6 octobre 2020.xq

Dans l'arrêt du 5 avril 2022, la CJUE précise que « [l]es États membres ont ainsi notamment la faculté de prendre des mesures de conservation visant des personnes faisant, au titre d'une telle identification, l'objet d'une enquête ou d'autres mesures de surveillance actuelles ou d'une inscription dans le casier judiciaire national mentionnant une condamnation antérieure pour des actes de criminalité grave pouvant impliquer un risque élevé de récidive. Or, lorsqu'une telle identification est fondée sur des éléments objectifs et non discriminatoires, définis par le droit national, la conservation ciblée visant des personnes ainsi identifiées est justifiée »⁵.

Par conséquent, l'article 1^{er}, point 1^o du projet de loi propose d'introduire un nouvel article 24-3 au Code de procédure pénale, qui permet au procureur d'État, dans le cadre de la recherche et de la poursuite d'infractions d'une certaine gravité, d'ordonner la conservation ciblée de données de trafic et de localisation suivant des conditions et critères déterminés conformément à la jurisprudence européenne.

A l'instar de l'article 25 de la loi belge du 20 juillet 2022 relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités (dénommée ci-après la « Loi belge du 20 juillet 2022 »), le libellé du nouvel article 24-3 introduit dès lors une conservation ciblée pour le futur de données relatives au trafic et à la localisation. Dès réception de l'ordonnance, les opérateurs et fournisseurs concernés doivent conserver les données demandées qu'ils génèrent ; il s'agit donc d'une sorte de « quick freeze » pour le futur.

Il échet de souligner dans ce contexte que l'ordonnance de conservation concerne la seule conservation des données, mais à ce moment, les autorités judiciaires n'ont pas encore accès aux données. Le but de la mesure est de préserver les données pour que les autorités judiciaires puissent y avoir accès ensuite par le biais et sous les conditions de l'article 67-1 du Code de procédure pénale.

Concernant plus particulièrement l'ordonnance de conservation, elle est ciblée en fonction de catégories de personnes concernées ou au moyen d'un critère géographique.

L'alinéa 3 du paragraphe 1^{er} indique la durée de la mesure de conservation et l'infraction qui fait l'objet de l'ordonnance. La durée de la mesure de conservation est limitée à six mois, renouvelable.

L'ordonnance doit également indiquer précisément la ou les personnes, le ou les lieux ainsi que les moyens de communications qui font l'objet de la conservation. Conformément à la jurisprudence européenne, la mesure ne concerne donc pas seulement les données afférentes au suspect, mais elle peut également viser des données afférentes à la victime, à son entourage social ou professionnel, à des lieux déterminés, tels que les lieux de la commission ou de la préparation de l'infraction, ou encore des moyens de communications. Le procureur d'Etat pourra ainsi, par exemple, ordonner la mesure de conservation des données pour un périmètre autour de la maison où il y a eu un assassinat, ainsi que pour les personnes qui connaissaient la victime.

L'ordonnance sera donc circonscrite à des éléments objectifs et non discriminatoires en précisant les personnes, les moyens de communication et les lieux auxquels la décision s'applique.

Le paragraphe 1^{er}, alinéa 2, de l'article 24-3 vise les catégories de données concernées et renvoie dans ce contexte au règlement grand-ducal du 24 juillet 2010 déterminant les catégories de données à caractère personnel générées ou traitées dans le cadre de la fourniture de services de communications électroniques ou de réseaux de communications publics.

Le paragraphe 3, alinéa 1^{er}, impose une obligation de confidentialité à toute personne qui a connaissance de la mesure. Cette obligation répond à un double objectif. D'une part, elle tient compte du bon déroulement de l'enquête afin que le suspect n'ait pas connaissance de l'enquête dont il est l'objet. Puis, la confidentialité permet également d'éviter que des personnes tentent de manipuler ou d'effacer des données à des fins de sécurité des données. Et finalement, la confidentialité de la mesure de conservation permet de contribuer à défendre le droit à la vie privée des personnes pouvant être concernées par ces données. Le libellé du paragraphe 3, alinéa 1^{er}, renvoie ainsi au secret professionnel.

Le paragraphe 3, alinéa 2, sanctionne le refus de collaboration et le libellé est inspirée de l'article 48-27 du Code de procédure pénale.

L'article 1^{er}, point 1^o du projet de loi propose également d'adapter la définition des fournisseurs concernés conformément à la terminologie utilisée à l'article 2 de la loi du 17 décembre 2021 sur les

⁵ Paragraphe 78 de l'arrêt du 5 avril 2022.

réseaux et les services de communications électroniques. Cette dernière a transposé en droit national la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen en élargissant le champ d'application de la législation sur les communications électroniques aux acteurs dits « OTT » (over-the-top players) en complément des services de communications classiques fondés sur la numérotation. Il s'agit notamment des services de messagerie tels que WhatsApp ou encore des appels vocaux-vidéo comme par exemple Skype ou Viber.

En remplaçant la notion de « *fournisseur d'un service de télécommunication* », telle que visée actuellement par les textes pertinents, par celle de « *fournisseur de services de communications électroniques* », l'article sous considération vise dès lors à se conformer aux dispositions du code de communications électroniques européen en harmonisant la législation nationale, d'une part, et à répondre à la nouvelle réalité technologique et l'évolution du secteur de communications électroniques, d'autre part.

La CJUE emploie d'ailleurs la même terminologie en référant notamment dans son dernier arrêt du 5 avril 2022 aux « *fournisseurs de services de communications électroniques* ». La nouvelle Loi belge du 20 juillet 2022 a également procédé à ladite adaptation de la terminologie conformément à la législation européenne.

La notion de « *fournisseur de services de communications électroniques* » est ainsi adaptée dans l'ensemble du projet de loi sous examen.

Ad Point 2° – article 48-27 du Code de procédure pénale :

En vue de l'introduction du nouvel article 10ter à la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques (dénommée ci-après la « Loi Telecom ») portant sur la conservation des données d'identification, la référence à l'article 10bis a été remplacée par celle de l'article 10ter, paragraphe 1^{er}. L'article 1^{er}, point 2° introduit un paragraphe 2 nouveau à l'article 48-27 du Code de procédure pénale portant sur l'accès du procureur d'État ou du juge d'instruction aux données conservées sur base de l'article 10ter, paragraphe 2, de la Loi Telecom, en vue de l'identification de l'utilisateur d'une adresse IP.

Il est renvoyé dans ce contexte aux commentaires sous l'article 2, point 9° du projet de loi.

Conformément aux explications données sous l'article 1^{er}, point 1° du projet de loi, l'article 1^{er}, point 2° du projet de loi adapte pareillement la définition des opérateurs et fournisseurs concernés à la lumière des autres dispositions proposées par le présent projet de loi.

Par analogie à cette modification terminologique, le projet de loi propose également de compléter la notion de « *télécommunications* » en incluant celle de « *communications électroniques* ». Cet ajout permet dès lors à tenir compte de l'actualité technologique du secteur de communications électroniques et d'adapter la législation nationale à l'évolution de la nouvelle réalité technologique qui ne se limite plus exclusivement au secteur classique des « *télécommunications* ».

Ad Point 3° – article 67-1 du Code de procédure pénale :

L'article 67-1 du Code de procédure pénale vise l'accès des autorités judiciaires aux données relatives au trafic et de localisation, conservées par les opérateurs et fournisseurs concernés conformément aux dispositions inscrites à la Loi Telecom ainsi que désormais au titre du nouvel article 24-3 du Code de procédure pénale proposé par le présent projet de loi.

L'article 67-1 du Code de procédure pénale avait déjà fait l'objet d'une proposition de modification par le projet de loi n° 6763 portant modification du Code d'instruction criminelle et de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques en réaction à l'arrêt rendu par la CJUE « Digital Rights Ireland » de 2014⁶. Or, suite aux nombreux arrêts subséquents de la CJUE, le texte proposé par ledit projet de loi ne répond plus aux exigences de la CJUE.

Dans son dernier arrêt du 5 avril 2022, la CJUE confirme sa jurisprudence selon laquelle, afin de garantir, en pratique, le plein respect des conditions strictes d'accès à des données à caractère personnel telles que les données relatives au trafic et à la localisation, l'accès des autorités nationales compétentes

6 CJUE, 8 avril 2014, Digital Rights Ireland et Seitlinger e.a. (affaires jointes C-293/12 et C-594/12).

aux données conservées doit être subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante, la décision de cette juridiction ou de cette entité devant intervenir à la suite d'une demande motivée de ces autorités présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénales. « *Ainsi, la Cour a notamment considéré qu'un ministère public qui dirige la procédure d'enquête et exerce, le cas échéant, l'action publique ne peut se voir reconnaître la qualité de tiers par rapport aux intérêts légitimes en cause, dès lors qu'il a pour mission non pas de trancher en toute indépendance un litige, mais de le soumettre, le cas échéant, à la juridiction compétente, en tant que partie au procès exerçant l'action pénale. Par conséquent, un tel ministère public n'est pas en mesure d'effectuer le contrôle préalable des demandes d'accès aux données conservées*⁷ ».

L'article 67-1 du Code de procédure pénale prévoit la possibilité d'accès aux données conservées par le juge d'instruction, de sorte que la disposition sous examen respecte la condition de contrôle préalable indépendant demandée par la CJUE et une modification afférente de l'article 67-1 n'est pas nécessaire.

Le Conseil d'Etat avait d'ailleurs déjà noté dans son avis du 10 juillet 2015⁸ concernant le projet de loi n° 6763 que « *[c]ette solution, retenue dès l'insertion de l'article 67-1 au Code d'instruction criminelle par la loi du 21 novembre 2002, est de nature à répondre – pour ce qui est de la transposition en droit national de la directive annulée – aux critiques formulées au regard des limitations des accès aux données retenues étant donné que l'ordonnance rendue par le juge d'instruction est susceptible de recours juridictionnels au vu de l'article 67-1, paragraphe 3, du Code d'instruction criminelle. La loi nationale prévoit ainsi des règles procédurales précises déterminant tant les accès que les recours contre ceux-ci. De même, le cercle des personnes pouvant recourir à cette mesure est déterminé par les dispositions sur l'organisation judiciaire, et est dès lors non seulement restreint, mais encore fermé.* »

Concernant les critères objectifs pour définir les circonstances et les conditions dans lesquelles doit être accordé aux autorités nationales compétentes l'accès aux données en cause, l'article 67-1 soumet d'ores et déjà l'accès aux données conservées à la condition préalable de faits qui « *emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement* ».

L'article 1^{er} du projet de loi n°6763 avait proposé de remplacer à l'article 67-1, le seuil de peine des infractions pour lesquelles les autorités répressives peuvent avoir recours aux données de communications retenues par les opérateurs par une liste d'infractions graves.

Dans son avis précité du 10 juillet 2015, « *[l]e Conseil d'État rappelle que, dans le cadre du projet de loi n° 6113, qui devait devenir la loi précitée du 24 juillet 2010, la question de l'insertion d'une liste au lieu d'un seuil de peine avait déjà fait l'objet de débats. Ainsi, on peut lire dans le rapport de la Commission parlementaire de l'enseignement supérieur, de la recherche, des médias et des communications que „quant à une liste des peines, telle que favorisée par exemple par la Commission nationale pour la protection des données et la Commission consultative des droits de l'homme dans leurs avis respectifs, les auteurs du projet de loi estiment que la détermination des infractions à retenir aurait été d'une complexité et d'une envergure énorme. Retenir uniquement les infractions d'actes de terrorisme et de criminalité organisée seraient un manquement grave dans le cadre de la lutte contre cette sorte d'infractions, puisque les infractions primaires ne seraient plus prises en considération. Selon les auteurs du projet de loi, le seuil de peine d'un an représente un compromis entre, d'une part, la recherche de l'efficacité du système, militant plutôt pour un seuil de peine relativement bas, et, d'autre part, la protection de la vie privée et des droits fondamentaux des citoyens, qui exigerait un seuil de peine plus élevé.“ Le Conseil d'État avait à l'époque exprimé sa préférence pour un seuil de peine, sans entrer plus amplement dans le débat entre les défenseurs d'un système de liste et les auteurs du projet de loi en question. La directive 2006/24/CE, en son article 4, avait laissé le choix aux États membres de déterminer selon leur droit national notamment „les conditions à remplir pour avoir accès aux données conservées dans le respect des exigences de nécessité et de proportionnalité“. Elle a été censurée sur ce point entre autres pour ne pas disposer „expressément que [l'] accès et l'utilisation [...] doivent être strictement restreints à des fins de prévention et de détection d'infractions graves précisément délimitées ou de poursuites pénales afférentes à celles-ci“. Le Conseil d'État n'en déduit*

⁷ Paragraphe 109 de l'arrêt du 5 avril 2022.

⁸ Document parlementaire n° 6763³.

pas la nécessité absolue pour le législateur national de devoir revenir sur sa décision initiale de procéder à une limitation par le recours à un seuil de peine. Tout au plus, mais il s'agit là d'un choix politique qui ne convient pas au Conseil d'État, pourrait-on vérifier si le seuil actuel d'un an doit être maintenu, ou bien s'il doit être porté à un niveau plus élevé, ainsi que cela avait été notamment discuté dans le cadre de la loi précitée du 24 juillet 2010. »

Dans ce contexte, il importe également de noter qu'il n'existe pas de définition autonome de la notion de « criminalité grave » dans le droit de l'Union européenne et la CJUE ne définit pas non plus ce qu'elle entend par criminalité grave dans ses arrêts récents. Il s'agit en effet plutôt d'une notion dynamique, qui se veut évolutive. Le projet de loi sous considération propose dès lors de ne pas établir une liste exhaustive d'infractions considérées de grave au vu de l'évolution de la criminalité en soi ainsi que des développements sociaux et de la politique pénale future.

La référence au seuil de peine des infractions est également le même modèle qui a été adopté en Belgique.

Tel qu'indiqué au document parlementaire n° 2572/001⁹, « [e]n Belgique, l'accès des autorités judiciaires aux données de trafic et de localisation à des fins de recherche, de détection et de poursuite d'infractions pénales d'une certaine gravité est réglementé par l'article 88bis du Code d'instruction criminelle. Outre des modalités procédurales et matérielles, des conditions d'accès y sont fixées dont le degré de gravité de l'infraction, qui justifie la mesure. Il y est, entre autres, prévu que le juge d'instruction puisse prendre la mesure uniquement s'il existe des indices sérieux que l'infraction est de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde, et lorsqu'il estime qu'il existe des circonstances qui rendent le repérage de communications électroniques ou la localisation de l'origine ou de la destination de communications électroniques nécessaire à la manifestation de la vérité. Par ailleurs, le juge d'instruction doit indiquer dans une ordonnance motivée les circonstances de fait de la cause qui justifient la mesure, son caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête. »

En outre, l'article 67-1, paragraphe 1^{er}, point 1. est complété par les termes « y inclus le repérage des adresses IP ». Etant donné que la jurisprudence européenne traite spécifiquement des adresses IP, séparément des données de trafic, il est proposé d'ajouter la mention spéciale de ces adresses IP au texte dans un souci de précision rédactionnelle et de sécurité juridique.

La terminologie visant les entités destinataires de l'ordonnance du juge d'instruction est adaptée et le projet de loi propose également de compléter la notion de « télécommunications » en incluant celle de « communications électroniques », conformément aux modifications effectuées à l'article 24-3 du Code de procédure pénale afin de répondre à la nouvelle réalité technologique. Il est partant renvoyé au commentaire de l'article 1^{er}, points 1^o et 2^o du projet de loi susmentionné.

Article 2 du projet de loi – modifications de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques:

Ad Point 1^o – article 2 de la Loi Telecom :

La définition du consentement inscrite à l'article 2 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques- (dénommée ci-après la « Loi Telecom ») vise à aligner la définition du « consentement » avec celle 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 (« règlement général sur la protection des données »).

Ad Point 2^o – article 3 de la Loi Telecom :

La loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel ayant été abrogée, le point 2^o propose de corriger la référence à l'article 3, paragraphe 1^{er}, alinéa 2, en visant désormais, à la lumière du point 1^o, le 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 (« règlement général sur la protection des données »).

⁹ Page 58 du document parlementaire n° 2572/001.

Ad Point 3° – article 5 de la Loi Telecom :

Dans son arrêt « Digital Rights Ireland » de 2014, la Cour de justice a invalidé la directive sur la conservation des données¹⁰ au motif que l'ingérence que comporte l'obligation générale de conservation des données relatives au trafic et des données de localisation imposée par celle-ci dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel n'était pas limitée au strict nécessaire.

Puis, dans son arrêt « Tele2 Sverige et Watson » de 2016¹¹, la Cour répond que le droit de l'Union européenne s'oppose à une réglementation nationale prévoyant une conservation généralisée et indifférenciée des données.

Par conséquent, l'article 2, point 3° du projet de loi prévoit l'introduction du principe d'interdiction d'une conservation généralisée et indifférenciée des données relatives au trafic tel que prévu actuellement à l'article 5. Le paragraphe 1^{er} de l'article 5 est partant supprimé et le paragraphe 2 devient le nouveau paragraphe 1^{er} dudit article 5.

Contrairement au libellé introduit par la Loi Telecom, qui a été modifié dernièrement par la loi du 24 juillet 2010, le principe inscrit au nouveau paragraphe 1^{er} est celui de l'interdiction de conservation des données relatives au trafic. Tel que prévu par la jurisprudence européenne, les données seront donc effacées ou rendues anonymes sur base du principe de nécessité et tel que préconisé par la CJUE¹².

Le projet de loi concerné vise ainsi à introduire un changement de perspective dans la conservation des données concernées, tel que demandé par la CJUE. Dans ce même contexte, la Cour constitutionnelle belge, dans son arrêt n°57/2021, faisant suite à l'arrêt « Quadrature du Net et FDN » et « Privacy International » de 2020, a invité le législateur belge à opérer un tel changement de principe, de sorte que la conservation des données demeure l'exception et non la règle.

En supprimant la possibilité de conservation généralisée et indifférenciée des données relatives au trafic et à la localisation, le présent projet de loi vise un tel changement de principe.

Cependant, même si la CJUE limite les possibilités de conservation généralisée et indifférenciée de données relatives au trafic, cette dernière demeure possible dans certains cas de figure, lorsque les dérogations à la protection des données à caractère personnel s'opèrent dans les limites du strict nécessaire. En effet, tel qu'expliqué aux commentaires des articles précédents, l'arrêt du 6 octobre 2020 autorise les exceptions au principe d'interdiction de tout stockage de masse de façon généralisée et indifférenciée :

- Les paragraphes 134 et suivants de l'arrêt visent les « *mesures législatives prévoyant la conservation préventive des données relatives au trafic et des données de localisation aux fins de la sauvegarde de la sécurité nationale* » (article 3 du projet de loi) ;
- Les paragraphes 152 et suivants de l'arrêt permettent les « *mesures législatives prévoyant la conservation préventive des adresses IP et des données relatives à l'identité civile aux fins de la lutte contre la criminalité et de la sauvegarde de la sécurité publique* » (article 2 du projet de loi).

Par ailleurs, l'arrêt de 2020 permet une conservation ciblée des données relatives au trafic et à la localisation en fonction de catégories de personnes concernées ou au moyen d'un critère géographique (article 2, point 4° du projet de loi) ainsi que la conservation rapide des données relatives au trafic et à la localisation dont disposent les opérateurs ou fournisseurs de services concernés (articles 1^{er} et 3 du projet de loi).

La modification du paragraphe 2, devenant le nouveau paragraphe 1^{er}, de l'article 5 vise dès lors la possibilité d'accès des seules autorités judiciaires et du Service de renseignement de l'Etat aux données qui ont été conservées selon les dispositions dérogoatoires au principe d'interdiction de conservation généralisée et indifférenciée des données relatives au trafic inscrit désormais au nouvel article 5 de la Loi Telecom.

10 Directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (JO L 105, p. 54).

11 CJUE, 21 décembre 2016, Tele2 (affaires C-203/15 et C-698/15).

12 Paragraphe 38 de l'arrêt du 5 avril 2022 : « *s'agissant du traitement et du stockage par les fournisseurs de services de communications électroniques des données relatives au trafic concernant les abonnés et les utilisateurs, (...) ces données doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication.* »

Le projet de loi propose également d'adapter la finalité d'accès aux données conservées tel que demandé par la jurisprudence européenne en remplaçant les mots de « *prévention, recherche, constatation et la poursuite des infractions pénales* » par ceux de la sauvegarde de « *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* ».

Ces finalités correspondent formellement à celles mentionnées par l'arrêt de 2020, qui relève aux points 142 et suivants qu' « *eu égard à la conciliation nécessaire des droits et des intérêts en cause, les objectifs de lutte contre la criminalité grave, de prévention d'atteintes graves à la sécurité publique et, a fortiori, de sauvegarde de la sécurité nationale sont susceptibles de justifier, compte tenu de leur importance, [...] l'ingérence particulièrement grave que comporte une conservation ciblée des données relatives au trafic et des données de localisation* ».

Ad Point 4° – article 5bis de la Loi Telecom :

Tel qu'expliqué au commentaire de l'article 2, point 3° du présent projet de loi, même si la CJUE limite les possibilités de conservation généralisée et indifférenciée de données relatives au trafic et à la localisation, cette dernière est autorisée dans certains cas de figure, à procéder à une conservation ciblée, notamment sur base géographique, afin de permettre aux autorités judiciaires et au Service de renseignement de l'Etat de remplir leurs missions.

Dans son arrêt du 6 octobre 2020, la CJUE a soumis la conservation ciblée sur base géographique aux conditions et critères suivants :

a) Concernant la **finalité** de la mesure :

« *Eu égard à la conciliation nécessaire des droits et des intérêts en cause, les objectifs de lutte contre la criminalité grave, de prévention d'atteintes graves à la sécurité publique et, a fortiori, de sauvegarde de la sécurité nationale sont susceptibles de justifier, compte tenu de leur importance, (...) l'ingérence particulièrement grave que comporte une conservation ciblée des données relatives au trafic et des données de localisation* »¹³.

L'article 5bis, paragraphe 1^{er}, alinéa 1^{er}, réfère dès lors à la finalité de « *sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention de menaces graves contre la sécurité publique* ».

b) Concernant la **durée** de la mesure :

« *Afin d'assurer que l'ingérence que comportent les mesures de conservation ciblée (...) soit conforme au principe de proportionnalité, leur durée ne saurait dépasser celle qui est strictement nécessaire au regard de l'objectif poursuivi ainsi que des circonstances les justifiant, sans préjudice d'un renouvellement éventuel en raison de la persistance de la nécessité de procéder à une telle conservation* »¹⁴.

L'article 5bis, paragraphe 1^{er}, alinéa 1^{er}, prévoit ainsi une durée maximale de six mois à partir de la date de la communication, à la lumière des anciens articles 5 et 9 de la Loi Telecom et dans un souci d'unification et d'harmonisation des durées de conservation.

c) Concernant les **données** à conserver :

Contrairement à l'article 2, point 9° du projet de loi, qui porte sur les données d'identification, l'article 2, point 4° sous considération vise les données relatives au trafic et à la localisation.

Il s'agit donc des mêmes données que celles qui étaient prévues aux anciens articles 5 et 9 de la Loi Telecom. L'article 5bis, paragraphe 1^{er}, alinéa 3 fait référence au règlement grand-ducal déterminant les catégories de données relatives au trafic et à la localisation, qui existe déjà ; il s'agit du règlement grand-ducal du 24 juillet 2010 déterminant les catégories de données à caractère personnel générées ou traitées dans le cadre de la fourniture de services de communications électroniques ou de réseaux de communications publics.

Le libellé de l'alinéa 2 est celui repris de l'article 5, paragraphe 1^{er}, point a), phrase 2, qui est toujours d'actualité et qui n'appelle pas d'autres observations.

¹³ Paragraphe 146 de l'arrêt du 6 octobre 2020.

¹⁴ Paragraphe 151 de l'arrêt du 6 octobre 2020.

- d) Concernant les **catégories de zones géographiques** où il peut y avoir une conservation des données:

Dans son arrêt du 6 octobre 2020, la CJUE a statué que « [l]a délimitation d'une mesure prévoyant la conservation des données relatives au trafic et des données de localisation peut également être fondée sur un critère géographique lorsque les autorités nationales compétentes considèrent, sur la base d'éléments objectifs et non discriminatoires, qu'il existe, dans une ou plusieurs zones géographiques, une situation caractérisée par un risque élevé de préparation ou de commission d'actes de criminalité grave. Ces zones peuvent être, notamment, des lieux caractérisés par un nombre élevé d'actes de criminalité grave, des lieux particulièrement exposés à la commission d'actes de criminalité grave, tels que des lieux ou infrastructures fréquentés régulièrement par un nombre très élevé de personnes, ou encore des lieux stratégiques, tels que des aéroports, des gares ou des zones de péages »¹⁵.

Les critères géographiques suggérés par la CJUE permettent ainsi de circonscrire les lieux caractérisés par un nombre élevé d'actes de criminalité grave, d'une part, et d'énumérer les lieux stratégiques, qui nécessitent de par leur nature (leur affectation, leur caractéristique ou leur symbolique) une protection, notamment via l'instauration d'une conservation de données sur ces lieux car ils pourraient être la cible d'actes de criminalité grave ou être exposés à des menaces pour la sécurité nationale, d'autre part.

L'article 5bis, paragraphe 2, vise la désignation des zones géographiques concernées, établie en fonction des hypothèses recommandées par la CJUE. Lesdites zones géographiques prévues sont celles inscrites à l'article 43bis, paragraphe 2, de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, dans le cadre du recours à la vidéosurveillance. Ladite disposition énumère les lieux qui, conformément à ce qui est également prescrit par la CJUE dans le contexte de la rétention des données, présentent un risque particulier de commission d'infractions pénales. La liste reprise à l'article 5bis, paragraphe 2, de la Loi Telecom a néanmoins été adaptée pour s'appliquer aux seuls 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.

Conformément à l'avis complémentaire du Conseil d'Etat du 12 mai 2020 relatif au projet de loi n° 7498, le point visant « les abords, les entrées et l'intérieur de l'enceinte du stade national de football et de rugby » n'a pas été repris, étant donné que le point qui vise « les lieux qui par leur nature rassemblent un grand nombre de personnes » que le point relatif aux « alentours et abords des infrastructures où sont organisés régulièrement des événements d'envergure nationale ou internationale » sont de nature à englober les lieux tels que le stade national de football et de rugby.

En plus de cette liste, et à l'image de l'article 126/3, paragraphe 2 de la loi belge du 13 juin 2005 relative aux communications électroniques, inséré par l'article 11 de la Loi belge du 20 juillet 2022, une conservation de toutes les zones géographiques est prévue au point 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, c'est-à-dire que la menace terroriste qui fait l'objet de l'analyse est vraisemblable et concrète.

Eu égard l'évolution constante de la criminalité grave et les capacités rapides d'adaptation des criminels, les différents facteurs d'émergence des crimes le projet de loi propose la détermination de l'étendue du périmètre de chaque zone géographique, par analogie à la désignation des infrastructures critiques au sens de la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale, sous forme d'un arrêté grand-ducal qui n'est pas publié obligatoirement, puisque la désignation a des implications pour la sécurité publique et la sécurité nationale. En effet, l'approche d'un arrêté grand-ducal pour l'étendue du périmètre de chaque zone, permettra aux autorités d'adapter plus facilement le périmètre des zones concernées, les évaluer ou bien y apporter des corrections, lorsque les évolutions de la société et de la criminalité le nécessitent ainsi que pour pouvoir s'adapter au contexte de la sécurité en rapide évolution. Concernant plus particulièrement cette évaluation des zones géographiques, il est renvoyé aux explications fournies au point e) ci-dessous.

¹⁵ Paragraphe 150 de l'arrêt du 6 octobre 2020.

Le paragraphe 3 de l'article 5bis prévoit des mesures techniques de mise en place d'une conservation ciblée des données relatives au trafic et de localisation selon les zones géographiques et suit les indications faites par les différents opérateurs concernés au cours d'une consultation informelle.

- e) Concernant l'évaluation des catégories de zones géographiques où il peut y avoir une conservation des données:

« Il convient encore de relever que les zones géographiques visées par une telle conservation ciblée peuvent et, le cas échéant, doivent être **modifiées** en fonction de l'évolution des conditions ayant justifié leur sélection, permettant ainsi notamment de réagir aux évolutions de la lutte contre la criminalité grave. »¹⁶

L'article 5bis, paragraphe 4, vise ainsi la création d'une commission qui proposera au Haut-Commissariat à la protection nationale l'étendue précise du périmètre de chaque zone géographique, d'une part, et elle procédera à l'évaluation de ces zones géographiques tous les trois ans en proposant le cas échéant les modifications nécessaires, d'autre part. Après la soumission de la proposition de ladite commission au Haut-Commissariat à la protection nationale, ce dernier transmettra la liste des zones géographiques avec l'étendue des périmètres aux opérateurs et fournisseurs concernés. Un rapport d'évaluation sera dressé tous les trois ans que le Haut-Commissariat à la protection nationale présente à la Chambre des députés.

Le libellé de ladite commission consultative a également été inspiré de la commission consultative en matière de vidéosurveillance prévue à l'article 43bis, paragraphe 3, de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale.

Enfin, l'article 5bis, paragraphe 5, propose l'introduction de sanctions pénales telles que prévues l'article 2, point 3° du projet de loi et par analogie aux anciens articles 5 et 9, paragraphe 6, de la Loi Telecom.

Ad Point 5° – article 5ter de la Loi Telecom :

Etant donné que l'obligation de conservation généralisée des données relatives au trafic et à la localisation a été supprimée aux articles 5 et 9 et que les dérogations de conservation généralisée ou ciblée des données à caractère personnel ont été partagées en différentes dispositions séparées, l'article 2, point 5° du projet de loi propose dès lors, dans un souci de cohérence, de modifier l'article 5-1, paragraphe 1^{er}, devenant le nouvel article 5ter de la Loi Telecom en remplaçant les mots « des articles 5 et 9 » par les mots « articles 5, 5bis et 9 ».

En plus, la référence désuète à la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel est remplacée par celle de la loi du 1^{er} 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.

Ad Point 6° – article 5quater de la Loi Telecom :

L'obligation de soumettre des statistiques à la Commission européenne a été vidée de sens par l'arrêt précité du 8 avril 2014 de la CJUE. Cependant, la Commission Nationale pour la Protection des Données a *de facto* régulièrement publié ces statistiques dans ses rapports annuels.

Etant donné que la publication de ces statistiques par la Commission Nationale pour la Protection des Données contribue à la transparence sur le sujet, il est proposé de consacrer cette pratique et de modifier l'article 5-2, devenant l'article 5quater nouveau de la Loi Telecom, de manière correspondante.

Ad Point 7° – article 7 de la Loi Telecom :

Le point 7° permet une mise à jour de l'article 7, paragraphe 5bis, de la Loi Telecom en l'adaptant au texte du Code européen des communications électroniques.

La loi du 19 décembre 2020 portant modification de la loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques et portant modification des articles 88-2

¹⁶ Paragraphe 82 de l'arrêt du 5 avril 2022.

et 88-4 du Code d'instruction criminelle a permis aux services de secours de localiser les personnes appelant le 112 (en situation d'urgence) via une fonctionnalité de leur smartphone.

Or depuis, la technologie ayant évolué, la référence aux seuls appels téléphoniques via les smartphones n'est plus suffisante et il faudrait également préciser le cadre légal pour les SMS d'urgence vers le 112. Dans ce même contexte, le Code européen des communications électroniques emploie également le terme de « communication d'urgence ». Par conséquent, le projet de loi sous considération profite de la présente modification afin de doter d'une base juridique claire les services d'urgence pour pouvoir recevoir les informations de localisation des personnes en situation d'urgence qui contactent le 112.

Ad Point 8° – article 9 de la Loi Telecom :

A l'instar de l'article 5 de la Loi Telecom, l'article 2, point 8° du projet de loi suggère de supprimer l'obligation de conservation généralisée des données de localisation autres que les données relatives au trafic et la finalité d'accès aux données conservées est adaptée aux critères de la jurisprudence européenne.

Il est renvoyé dans ce contexte aux explications énoncées au commentaire de l'article 2, point 3° du projet de loi.

Ad Point 9° – article 10ter de la Loi Telecom :

Alors que la jurisprudence européenne interdit la conservation généralisée et indifférenciée des données relatives au trafic et à la localisation, la CJUE ne s'oppose pas à des mesures législatives prévoyant une conservation généralisée et indifférenciée des données d'identification et des adresses IP attribuées à la source d'une communication, pour autant que la durée de conservation est limitée au strict nécessaire.

En effet, dans le dispositif de son arrêt du 6 octobre 2020, la CJUE souligne qu'elle ne s'oppose pas à des mesures législatives prévoyant :

- « – *aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire ;*
- *aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité et de la sauvegarde de la sécurité publique, une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques ».*

La CJUE opère ainsi une distinction entre :

- la conservation généralisée et indifférenciée des adresses IP attribuées à une source de connexion, laquelle peut être imposée aux opérateurs par la législation uniquement aux fins de sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, et ce pour une période temporellement limitée au strict nécessaire, et,
- la conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, laquelle peut être imposée aux opérateurs par la législation à des fins plus larges, à savoir la sauvegarde de la sécurité nationale, la lutte contre la criminalité, que celle-ci soit grave ou non, et la sauvegarde de la sécurité publique, même lorsque cette sécurité ne fait pas l'objet de menaces graves, et ce sans que ces données doivent être conservées pour une période temporelle limitée au strict nécessaire.

Par conséquent, l'article 10ter nouveau est scindé en deux paragraphes distinguant entre les données relatives à l'identité civile au paragraphe 1^{er}, d'une part, et les adresses IP au paragraphe 2, d'autre part.

a) Concernant plus particulièrement **les données relatives à l'identité civile** :

Selon l'arrêt de la CJUE du 6 octobre 2020, « *les données relatives à l'identité civile des utilisateurs des moyens de communications électroniques, (...) ne permettent pas, à elles seules, de connaître la date, l'heure, la durée et les destinataires des communications effectuées, non plus que les endroits où ces communications ont eu lieu ou la fréquence de celles-ci avec certaines personnes pendant une période donnée, de telle sorte qu'elles ne fournissent, mises à part les coordonnées de ceux-ci, telles que leurs adresses, aucune information sur les communications données et, par voie de*

conséquence, sur leur vie privée. Ainsi, l'ingérence que comporte une conservation de ces données ne saurait, en principe, être qualifiée de grave. Il en découle que (...) les mesures législatives visant le traitement de ces données en tant que telles, notamment leur conservation et l'accès à celles-ci à la seule fin de l'identification de l'utilisateur concerné, et sans que lesdites données puissent être associées à des informations relatives aux communications effectuées, sont susceptibles d'être justifiées par l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général (...). Dans ces conditions (...) il y a lieu de considérer que, même en l'absence de lien entre l'ensemble des utilisateurs des moyens de communications électroniques et les objectifs poursuivis, (...) la Charte, ne s'oppose pas à une mesure législative imposant, sans délai particulier, aux fournisseurs de services de communications électroniques la conservation des données relatives à l'identité civile de l'ensemble des utilisateurs des moyens de communications électroniques aux fins de la prévention, de la recherche, de la détection et de la poursuite d'infractions pénales ainsi que de la sauvegarde de la sécurité publique, sans qu'il soit nécessaire que les infractions pénales ou que les menaces contre ou les atteintes à la sécurité publique soient graves »¹⁷.

La CJUE autorise partant les Etats membres à imposer aux opérateurs et fournisseurs concernés la conservation des données relatives à l'identité civile. Ces données d'identification ne donnent effectivement pas d'information sur la communication en soi, ni sur son contenu, ni sur la localisation précise de l'individu concerné. Elles sont donc moins intrusives dans la vie privée que les données relatives au trafic et à la localisation, c'est-à-dire les métadonnées.

Actuellement, la loi du 27 juin 2018 adaptant la procédure pénale aux besoins liés à la menace terroriste crée un fichier centralisé auprès de l'Institut Luxembourgeois de Régulation dans lequel les opérateurs doivent mettre à disposition les données de souscription des abonnés telles que prévues à l'article 10bis de la Loi Telecom. La loi du 7 juin 2017 portant modification de la loi du 27 février 2011 sur les réseaux et les services de communications électroniques vise, quant à elle, la collecte et la conservation des données à caractère personnel des clients d'un service à prépaiement.

Or, compte tenu de la convergence croissante des services de communications électroniques et de l'extension de cette dernière notion, ainsi que de la notion d'opérateur aux acteurs « OTT », à la suite de la transposition du code des communications électroniques européen, il est proposé d'adapter la liste des données d'identification à conserver au-delà des données visées à l'article 10bis de la Loi Telecom. Il s'agit plus particulièrement des données qui suivent :

- Les données de souscription de l'abonné ainsi que les données d'identification de l'utilisateur final ou le service de communications électroniques employé :

Avec les évolutions et en particulier le développement des médias sociaux, « *le nom, le prénom, le lieu de résidence habituelle, la date et le lieu de naissance ainsi que le numéro de contact de l'abonné* » exigé par l'article 10bis de la Loi Telecom ne sont plus les seuls moyens utiles pour identifier une personne. Par ailleurs, des personnes mal intentionnées parviennent à s'identifier sous un faux nom ou bien un document d'identité falsifié par exemple et des données supplémentaires s'avèrent nécessaires afin de pouvoir procéder à retrouver la véritable identité de l'abonné ou bien l'utilisateur effectif du service.

Déterminer l'identité d'une personne est la plupart du temps la première démarche de toute approche des autorités judiciaires et du Service de renseignement de l'Etat dans le cadre d'une enquête et le recours aux données d'identification listées au nouvel article 10ter s'avère dès lors souvent crucial.

- 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 :

Contrairement aux adresses IP à la source de la connexion qui sont traitées séparément au paragraphe 2, les adresses IP ayant servi à la souscription ou à l'activation du service de communication électronique sont des données d'identification telles que pour une télécommunication classique.

Par ailleurs, la conservation de l'adresse IP en soi n'est pas suffisante pour atteindre l'objectif poursuivi de l'identification de l'utilisateur final et effectif. En effet, il est nécessaire de conserver également le port source de la connexion et l'horodatage. Pour des raisons techniques et commerciales, bon nombre de fournisseurs concernés ont migré vers le partage d'une adresse IP entre

¹⁷ Paragraphes 157, 158 et 159 de l'arrêt du 6 octobre 2020.

plusieurs utilisateurs finaux. La conservation des ports source de la connexion et de l'horodatage a donc pour but de différencier les différents utilisateurs finaux partageant une même adresse IP et d'identifier de manière univoque et non ambiguë l'utilisateur final impliqué (c'est-à-dire le suspect).

- L'identité internationale d'abonné mobile (IMSI) :

L'IMSI est un identifiant qui se trouve dans la carte SIM et qui permet d'identifier de manière unique chaque abonné.

- L'identité internationale d'équipement mobile (IMEI) :

L'IMEI est un numéro d'identification unique qui permet d'immatriculer un équipement mobile. L'IMEI constitue une donnée essentielle à l'identification de l'auteur présumé d'une infraction. En pratique, on observe que, surtout dans des affaires de stupéfiants, les auteurs d'infractions changent de cartes SIM et les placent dans un seul et même appareil pour communiquer. Le numéro IMEI de l'équipement terminal est ainsi indispensable dans le cadre de l'enquête ou de l'instruction.

Puis, si une certaine carte SIM est enregistrée sous un faux nom, mais qu'elle est utilisée dans un appareil auquel peut être associée une seconde carte SIM dont le titulaire est correctement identifié, cela donne une indication sur la véritable identité de l'utilisateur de la première carte SIM.

Il échet de noter dans ce contexte que l'IMSI et l'IMEI ne permettent donc pas le traçage du parcours de navigation d'un utilisateur, qui serait couvert par la mesure de repérage, mais elle sert exclusivement à des fins d'identification.

L'accès à l'ensemble de ces données se limite, pour les autorités judiciaires, aux mesures prévues à l'article 48-27 du Code de procédure pénale et, pour le Service de renseignement de l'Etat, à celles prises dans le cadre de la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État.

b) Concernant plus particulièrement **les données relatives aux adresses IP**:

Dans les paragraphes 152 et suivants de l'arrêt de la CJUE du 6 octobre 2020, il est relevé que « les adresses IP, quoique faisant partie des données relatives au trafic, sont générées sans être rattachées à une communication déterminée et servent principalement à identifier, par l'intermédiaire des fournisseurs de services de communications électroniques, la personne physique propriétaire d'un équipement terminal à partir duquel une communication au moyen de l'Internet est effectuée. Ainsi, en matière de courrier électronique ainsi que de téléphonie par Internet, pour autant que seules les adresses IP de la source de la communication sont conservées et non celles du destinataire de celle-ci, ces adresses ne révèlent, en tant que telles, aucune information sur les tierces personnes ayant été en contact avec la personne à l'origine de la communication. Cette catégorie de données présente donc un degré de sensibilité moindre que les autres données relatives au trafic. Toutefois, les adresses IP pouvant être utilisées pour effectuer notamment le traçage exhaustif du parcours de navigation d'un internaute et, par suite, de son activité en ligne, ces données permettent d'établir le profil détaillé de ce dernier. Ainsi, la conservation et l'analyse desdites adresses IP que nécessite un tel traçage constituent des ingérences graves dans les droits fondamentaux de l'internaute (...). Or, aux fins de la conciliation nécessaire des droits et des intérêts en cause exigée par la jurisprudence (...), il y a lieu de tenir compte du fait que, dans le cas d'une infraction commise en ligne, l'adresse IP peut constituer le seul moyen d'investigation permettant l'identification de la personne à laquelle cette adresse était attribuée au moment de la commission de cette infraction. À cela s'ajoute le fait que la conservation des adresses IP par les fournisseurs de services de communications électroniques au-delà de la durée d'attribution de ces données n'apparaît, en principe, pas nécessaire aux fins de la facturation des services en cause, de telle sorte que la détection des infractions commises en ligne peut, de ce fait, (...) s'avérer impossible sans avoir recours à une mesure législative (...). Tel peut notamment être le cas, (...) des infractions particulièrement graves en matière de pédopornographie (...). Dans ces conditions, s'il est vrai qu'une mesure législative prévoyant la conservation des adresses IP de l'ensemble des personnes physiques propriétaires d'un équipement terminal à partir duquel un accès à Internet peut être effectué viserait des personnes qui ne présentent, de prime abord, pas de lien, (...) avec les objectifs poursuivis (...), une mesure législative prévoyant la conservation généralisée et indifférenciée des seules adresses IP attribuées à la source d'une connexion n'apparaît pas, en principe, contraire à (...) la Charte, pourvu que cette possibilité soit soumise au strict respect des conditions matérielles et procédurales devant régir l'utilisation de ces données. »

De la même façon que les données d'identification, la CJUE autorise donc les Etats membres à imposer aux opérateurs et fournisseurs concernés la conservation des adresses IP à la source de la connexion.

L'article 2, point 9° du projet de loi créant un nouvel article 10^{ter}, paragraphe 2, vise partant la conservation de ces données relatives aux adresses IP à la source de la connexion tout en répondant aux conditions régies par la jurisprudence européenne.

En effet, l'adresse IP à la source de la connexion est essentielle dans le cadre des enquêtes judiciaires ainsi que pour le Service de renseignement de l'Etat, qui peuvent y accéder respectivement conformément à l'article 48-27 du Code de procédure pénale et la loi du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État. L'adresse IP à la source d'une connexion va, par exemple, aider à identifier la personne qui a transmis des messages de menace de mort envoyés vers une victime, ou va aider à identifier la personne qui est l'auteur du message fixant rendez-vous à une fille mineure portée disparue.

A l'instar des adresses IP ayant servi à la souscription ou à l'activation du service de communication électronique, l'identification des adresses IP à la source de la connexion ne permet pas d'effectuer, à elle seule, le traçage du parcours de navigation d'une personne ou de son activité en ligne. Elles servent principalement à identifier, par l'intermédiaire des fournisseurs concernés, la personne physique propriétaire d'un équipement terminal à partir duquel une communication au moyen de l'Internet est effectuée, tel qu'autorisé par la CJUE. Le traçage du parcours de navigation ainsi que l'adresse IP de destination pourront uniquement être demandés dans le cadre d'une demande de repérage qui sera désormais entourée de conditions et de critères strictes conformément à la jurisprudence européenne.

- Concernant la **finalité** de la mesure :

*« Eu égard au caractère grave de l'ingérence dans les droits fondamentaux (...), seule la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique sont de nature, à l'instar de la sauvegarde de la sécurité nationale, à justifier cette ingérence. »*¹⁸

L'article 10^{ter}, paragraphe 2, alinéa 1^{er}, limite dès lors la mesure de conservation aux seuls *« 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 »*.

- Concernant la **durée** de la mesure :

*« En outre, la durée de conservation ne saurait excéder celle qui est strictement nécessaire au regard de l'objectif poursuivi. »*¹⁹

L'article 10^{ter}, paragraphe 2, prévoit ainsi la durée maximale de conservation des données de six mois. La durée de conservation de six mois correspond à la durée de conservation strictement nécessaire pour permettre aux autorités de mener à bien leurs enquêtes, en particulier en matière de lutte contre la criminalité grave.

Il importe de souligner que pour des raisons techniques, ces données visent l'adresse IP source, mais aussi 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. Il est renvoyé dans ce contexte aux explications fournies pour l'article 10^{ter}, paragraphe 1^{er}.

Finalement, le paragraphe 3 propose l'introduction de sanctions pénales par analogie aux anciens articles 5 et 9, paragraphe 6, de la Loi Telecom.

Ad Point 10° – article 12 de la Loi Telecom :

A la lumière des points 1° et 2°, le point 10° met également à jour la référence à la loi du 1^{er} août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, ce qui n'appelle pas d'autres observations.

¹⁸ Paragraphe 159 de l'arrêt du 6 octobre 2020.

¹⁹ Paragraphe 159 de l'arrêt du 6 octobre 2020.

Article 3 du projet de loi – modifications de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat:

Ad Point 1° – article 7 de la Loi SRE :

L'article 3, point 1° du projet de loi adapte la définition des opérateurs et fournisseurs concernés à la lumière des autres dispositions proposées par le présent projet de loi et il est renvoyé aux explications données sous l'article 1^{er}, point 1° du projet de loi.

Il échet de noter dans ce contexte que l'article 3, point 11°/1 de la loi organique des services de renseignement et de sécurité belges du 30 novembre 1998 réfère à la même terminologie en définissant le « *fournisseur d'un service de communications électroniques* » comme « *quiconque qui, de quelque manière que ce soit, met à disposition ou offre, sur le territoire belge, un service qui consiste en la transmission de signaux via des réseaux de communications électroniques ou qui permet aux utilisateurs, via un réseau de communications électroniques, d'obtenir, de recevoir ou de diffuser des informations* ».

Ad Point 2° – article 7-1 de la Loi SRE :

Tel qu'expliqué précédemment, la CJUE confirme que le droit de l'Union s'oppose à une réglementation nationale imposant à un fournisseur de services de communications électroniques, à des fins de lutte contre les infractions en général ou de sauvegarde de la sécurité nationale, la transmission ou la conservation généralisée et indifférenciée de données relatives au trafic et à la localisation. En revanche, dans des situations dans lesquelles un État membre fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, celui-ci peut déroger à l'obligation d'assurer la confidentialité des données afférentes aux communications électroniques en imposant, par des mesures législatives, une conservation généralisée et indifférenciée de ces données pour une durée temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de la menace.

La Cour rappelle que la « *directive vie privée et communications électroniques* » ne permet pas que la dérogation à l'obligation de principe de garantir la confidentialité des communications électroniques et des données y afférentes et à l'interdiction de stocker ces données devienne la règle. Ceci implique que cette directive n'autorise les États membres à adopter, entre autres à des fins de sécurité nationale, des mesures législatives visant à limiter la portée des droits et des obligations prévus par cette directive, notamment l'obligation de garantir la confidentialité des communications et des données relatives au trafic, que dans le respect des principes généraux du droit de l'Union, parmi lesquels figure le principe de proportionnalité, et des droits fondamentaux garantis par la Charte.

Dans ce cadre, la Cour considère, d'une part, dans l'arrêt du 6 octobre 2020, que la directive « *vie privée et communications électroniques* », lue à la lumière de la Charte, s'oppose à une réglementation nationale, imposant aux fournisseurs de services de communications électroniques, en vue de la sauvegarde de la sécurité nationale, la transmission généralisée et indifférenciée aux services de sécurité et de renseignement des données relatives au trafic et à la localisation. D'autre part, elle estime que cette même directive s'oppose à des mesures législatives imposant aux fournisseurs de services de communications électroniques, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation. En effet, ces obligations de transmission et de conservation généralisée et indifférenciée de telles données constituent des ingérences particulièrement graves dans les droits fondamentaux garantis par la Charte, sans que le comportement des personnes dont les données sont concernées présente de lien avec l'objectif poursuivi par la réglementation en cause. De manière analogue, la Cour interprète l'article 23, paragraphe 1^{er}, du règlement général sur la protection des données, lu à la lumière de la Charte, en ce sens qu'il s'oppose à une réglementation nationale imposant aux fournisseurs d'accès à des services de communication au public en ligne et aux fournisseurs de services d'hébergement la conservation généralisée et indifférenciée, notamment, des données à caractère personnel afférentes à ces services.

En revanche, la Cour estime que, dans des situations où l'État membre concerné fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, la directive « *vie privée et communications électroniques* », lue à la lumière de la Charte, ne s'oppose pas au fait d'enjoindre aux fournisseurs de services de communications électroniques de conserver de manière généralisée et indifférenciée des données relatives au trafic et à la localisation. Dans ce contexte, la Cour précise que la décision prévoyant cette injonction, pour une période temporellement limitée au strict nécessaire, doit faire l'objet d'un contrôle effectif, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, afin de vérifier l'existence d'une

de ces situations ainsi que le respect des conditions et des garanties prévues. Dans ces mêmes conditions, ladite directive ne s'oppose pas non plus à l'analyse automatisée des données, notamment celles relatives au trafic et à la localisation, de l'ensemble des utilisateurs de moyens de communications électroniques.

Selon la CJUE, la Charte des droits fondamentaux de l'Union européenne (dénommée ci-après la « Charte ») admet des limitations au principe de confidentialité des communications électroniques et des données relatives au trafic y afférentes « pour autant que ces limitations soient prévues par la loi (...) et que, dans le respect du principe de proportionnalité, elles soient nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui²⁰ ». A cet égard, la CJUE a jugé dans son arrêt du 6 octobre 2020 que « l'importance de l'objectif de sauvegarde de la sécurité nationale (...) dépasse celle des autres objectifs visés (...), notamment des objectifs de lutte contre la criminalité en général, même grave, ainsi que de sauvegarde de la sécurité publique. » L'objectif de sauvegarde de la sécurité nationale « est dès lors susceptible de justifier des mesures comportant des ingérences dans les droits fondamentaux plus graves que celles que pourraient justifier ces autres objectifs²¹ ».

C'est ainsi que la CJUE admet des mesures législatives autorisant « les autorités compétentes à enjoindre aux fournisseurs de services de communications électroniques de procéder à la conservation des données relatives au trafic et des données de localisation de l'ensemble des utilisateurs des moyens de communications électroniques pendant une période limitée, dès lors qu'il existe des circonstances suffisamment concrètes permettant de considérer que l'Etat membre concerné fait face à une menace grave (...) pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible. Même si une telle mesure vise, de manière indifférenciée, tous les utilisateurs de moyens de communications électroniques sans que ceux-ci paraissent, de prime abord, présenter de rapport (...) avec une menace pour la sécurité nationale de cet Etat membre, il y a lieu néanmoins de considérer que l'existence d'une telle menace est de nature, par elle-même, à établir ce rapport²² ».

L'article 3, point 2° du projet de loi introduit dès lors un nouvel article 7-1 à la Loi SRE qui vise la conservation des données de trafic et de localisation sous strictes conditions établies conformément à la jurisprudence européenne :

- Concernant **la durée** de la mesure :

Concernant plus particulièrement les critères de cette conservation des données, l'arrêt du 6 octobre 2020 prévoit que l'injonction doit « être temporellement limitée au strict nécessaire. S'il ne peut être exclu que l'injonction (...) puisse, en raison de la persistance d'une telle menace, être renouvelée, la durée de chaque injonction ne saurait dépasser un laps de temps prévisible²³ ». C'est ainsi que l'article 7-1, paragraphe 4, prévoit une durée de conservation limitée à six mois. Cette durée de six mois peut être prolongée en cas de persistance de la menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible et en suivant la même procédure d'autorisation prévue au paragraphe 2 de l'article 7-1. Le paragraphe 4, alinéa 2 de l'article 7-1 impose également la fin de la conservation lorsque la menace cesse ou si la conservation n'est plus nécessaire.

- Concernant **le contrôle** de la mesure :

Le paragraphe 138 de l'arrêt précité de 2020 précise également que la conservation « ne saurait présenter un caractère systématique ». A cette fin, le paragraphe 5 du nouvel article 7-1 prévoit que le directeur du SRE soumet une fois par mois, un rapport écrit au Comité ministériel de renseignement sur l'évolution de la menace et justifiant, le cas échéant, le maintien ou la fin de la conservation des données concernées. Cette disposition entend ainsi également à répondre à la demande de la CJUE que « la décision faisant injonction aux fournisseurs de services de communications électroniques de procéder à une telle conservation des données puisse faire l'objet d'un contrôle effectif soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier (...) le respect des conditions et des garanties devant être prévues »²⁴.

20 Paragraphe 48 de l'arrêt du 5 avril 2022.

21 Paragraphe 136 de l'arrêt du 6 octobre 2020.

22 Paragraphe 137 de l'arrêt du 6 octobre 2020.

23 Paragraphe 138 de l'arrêt du 6 octobre 2020.

24 Paragraphe 139 de l'arrêt du 6 octobre 2020.

Il échet de souligner dans ce contexte que l'article 24, paragraphe 3 de la loi organique du SRE prévoit un contrôle à posteriori des activités du SRE en disposant que la « *commission de contrôle parlementaire peut procéder à des contrôles portant sur des dossiers spécifiques. À cette fin, la commission de contrôle parlementaire est autorisée à prendre connaissance de tous les informations et renseignements et de toutes pièces qu'elle juge pertinentes pour l'exercice de sa mission, à l'exception d'informations et de renseignements ou de pièces susceptibles de révéler l'identité d'une source du SRE ou pouvant porter atteinte aux droits de la personne d'un tiers.* »

Le libellé de l'article 7-1, est inspiré de l'article 34 de la Loi belge du 20 juillet 2022.

Finalement, le paragraphe 6, sanctionne le refus de collaboration à la lumière de l'article 1^{er}, point 1^o du projet de loi et il est dès lors renvoyé aux explications fournies pour ladite disposition.

Ad Point 3^o – article 7-2 de la Loi SRE :

L'arrêt de la CJUE du 6 octobre 2020 permet pour des finalités de lutte contre la criminalité grave et la sauvegarde de la sécurité nationale, une législation permettant une conservation rapide des données relatives au trafic et des données de localisation²⁵.

Au paragraphe 91 de l'arrêt de la CJUE du 5 avril 2022, la Cour relève que la directive « vie privée et communications électroniques » ne s'oppose pas à ce que les autorités nationales compétentes ordonnent une mesure de conservation rapide dès le premier stade de l'enquête portant sur une menace grave pour la sécurité publique ou sur un éventuel acte de criminalité grave, à savoir à partir du moment auquel ces autorités peuvent, selon les dispositions pertinentes du droit national, ouvrir une telle enquête. Une telle mesure peut être étendue aux données relatives au trafic et aux données de localisation afférentes à des personnes autres que celles qui sont soupçonnées d'avoir projeté ou commis une infraction pénale grave ou une atteinte à la sécurité nationale, pour autant que ces données puissent, sur la base d'éléments objectifs et non discriminatoires, contribuer à l'élucidation d'une telle infraction ou d'une telle atteinte à la sécurité nationale, telles que les données de la victime de celle-ci ainsi que celles de son entourage social ou professionnel.

La Cour a également précisé au paragraphe 88 de l'arrêt précité de 2022, que ladite « *mesure de conservation de cette nature ne doit pas être limitée aux données des personnes identifiées préalablement comme présentant une menace pour la sécurité publique ou la sécurité nationale de l'Etat membre concerné ou des personnes concrètement soupçonnées d'avoir commis un acte de criminalité grave ou une atteinte à la sécurité nationale. En effet, selon la Cour, (...) une telle mesure peut, (...) être étendue aux données relatives au trafic et aux données de localisation afférentes à des personnes autres que celles qui sont soupçonnées d'avoir projeté ou commis une infraction pénale grave ou une atteinte à la sécurité nationale, pour autant que ces données puissent, sur la base d'éléments objectifs et non discriminatoires, contribuer à l'élucidation d'une telle infraction ou d'une telle atteinte à la sécurité nationale, telles que les données de la victime de celle-ci ainsi que celles de son entourage social ou professionnel* ».

L'article 3, point 3^o du projet de loi propose ainsi l'introduction de la possibilité pour le SRE de demander la conservation ciblée des données relatives au trafic et à la localisation suivant des conditions et critères déterminés conformément à la jurisprudence européenne.

Plus particulièrement, le nouvel article 7-2 introduit dès lors un « quick freeze » qui permet au SRE d'ordonner une conservation rapide de données relatives à une cible déterminée lorsque cela s'impose pour protéger la sécurité nationale ainsi qu'une conservation ciblée pour le futur de données.

a) Concernant plus particulièrement l'injonction de conservation des données déjà générées – « **quick freeze** » :

Le point 1^o du nouvel article 7-2, paragraphe 1^{er}, de la Loi SRE prévoit dès lors que l'opérateur ou le fournisseur de services concerné est tenu de conserver les données qu'il possède déjà au moment de l'injonction. Il s'agit donc de données qui ont dû être conservées par exemple sur base de l'article 2, point 4^o du présent projet de loi (conservation des données de trafic ou de localisation dans certaines zones géographiques) ou conformément au nouvel article 7-1 de la Loi SRE susmentionné. Dans l'intérêt des missions du SRE au sens de l'article 3 de la Loi SRE, l'opérateur ou le fournisseur de services concerné peut dès lors être requis de « sécuriser » et de conserver lesdites données historiques disponibles pour une durée de six mois, renouvelable.

²⁵ Paragraphes 160 et suivants de l'arrêt du 6 octobre 2020.

L'accès à ces données conservées se fera selon la procédure inscrite à l'article 7, paragraphe 2, de la Loi SRE après avoir recueilli les autorisations et assentiments nécessaires.

Tel qu'expliqué ci-dessus, un contrôle à posteriori des injonctions de conservation restera de mise suivant l'article 24 de la Loi SRE portant sur la commission de contrôle parlementaire.

- b) Concernant plus particulièrement l'injonction de conservation des données générées à partir de la date d'injonction – « *freeze futur* » :

Le point 2° du nouvel article 7-2, paragraphe 1^{er}, de la Loi SRE prévoit que l'opérateur ou le fournisseur de services concerné est tenu de conserver les données générées à dater de la réception de l'injonction. Il s'agit donc de données futures et l'opérateur ou le fournisseur de services concerné peut dès lors être requis de « sécuriser » et de conserver lesdites données pour une durée de six mois à partir de l'injonction, renouvelable.

Dans les deux cas, le paragraphe 2 prévoit que l'injonction adressée à l'opérateur ou le fournisseur concerné mentionne clairement quelles données de trafic et de localisation doivent être conservées en vue d'une conservation ciblée et différenciée. Les éléments mentionnés dans l'injonction sont des données d'identification des personnes ou groupes de personnes visés, des caractéristiques techniques (numéro d'appel, IMSI, IMEI par exemple) et/ou une localisation précise.

Lorsque le SRE ne dispose que d'informations relatives à un mode d'utilisation particulier de moyens de communications, une injonction pourra également être émise. Il s'agit par exemple de l'hypothèse des enquêtes d'espionnage lors desquelles des « *burner phones* » peuvent être détectés grâce à une combinaison de caractéristiques techniques, géographiques et temporelles (pour contacter des sources clandestines).

Le paragraphe 3 propose à ce que s'il est mis fin à la mesure, le SRE en informe immédiatement l'opérateur ou le fournisseur concerné afin que la conservation des données prenne fin.

Le paragraphe 4 prévoit, par analogie à l'article 7-1, paragraphe 5, précité ainsi qu'à l'article 5, paragraphe 3, de la Loi SRE portant sur les observations, un contrôle mensuel des injonctions de conservation par le Comité ministériel du renseignement. Un contrôle effectif à posteriori des injonctions de conservation s'appliquera également toujours suivant l'article 24 de la Loi SRE visant la commission de contrôle parlementaire. Le projet de loi garanti ainsi le respect de la considération de la CJUE que « *[l]orsque ce contrôle est effectué non par une juridiction, mais par une entité administrative indépendante, celle-ci doit jouir d'un statut lui permettant d'agir lors de l'exercice de ses missions de manière objective et impartiale et doit être, à cet effet, à l'abri de toute influence extérieure. Ainsi, l'exigence d'indépendance à laquelle doit satisfaire l'entité chargée d'exercer le contrôle préalable impose que celle-ci ait la qualité de tiers par rapport à l'autorité qui demande l'accès aux données, de sorte que ladite entité soit en mesure d'exercer ce contrôle de manière objective et impartiale, en étant protégée de toute influence extérieure. En particulier, dans le domaine pénal, l'exigence d'indépendance implique que l'autorité chargée de ce contrôle préalable, d'une part, ne soit pas impliquée dans la conduite de l'enquête pénale en cause et, d'autre part, ait une position de neutralité à l'égard des parties à la procédure pénale* »²⁶.

L'accès à ces données conservées se fera également selon la procédure inscrite à l'article 7, paragraphe 2, de la Loi SRE après avoir recueilli les autorisations et assentiments nécessaires.

Finalement, de manière identique à l'article 7-1, paragraphe 6, ci-dessus, l'article 7-2, paragraphe 5, sanctionne le refus de collaboration et il est dès lors renvoyé aux explications fournies à l'article 1^{er}, point 1° du projet de loi.

Article 4 du projet de loi – disposition transitoire :

Afin que les opérateurs et fournisseurs concernés puissent mettre en pratique la conservation ciblée des données relatives au trafic et à la localisation selon les zones géographiques, telles que prévues à l'article 2, point 4° du projet de loi, ils doivent disposer au préalable de la liste précise de l'étendue du périmètre des zones concernées. Par conséquent, avant de mettre en œuvre cette conservation ciblée et d'effacer les autres données de trafic et de localisation qui, conformément aux articles 5 et 9 de la Loi Telecom, ne peuvent plus être conservées, la commission consultative devra commencer ses travaux en priorité.

²⁶ Paragraphe 108 de l'arrêt du 5 avril 2022.

L'article 4 du projet de loi prévoit partant que ladite commission consultative présentera 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 loi au Journal officiel du Grand-Duché de Luxembourg. Suite à la communication de l'arrêté grand-ducal y afférent aux opérateurs et fournisseurs concernés, ces derniers disposeront d'un délai restant de neuf mois afin de prendre les mesures techniques et organisationnelles nécessaires pour procéder à la mise en place de la conservation ciblée et de la suppression des données résiduelles non visées par ladite conservation.

Article 5 du projet de loi – intitulé du projet de loi :

L'article 3 autorise la mention de la loi future dans d'autres textes normatifs moyennant une formule abrégée, ce qui n'appelle pas d'autres observations.

Article 6 du projet de loi – entrée en vigueur :

L'article 6, alinéa 1^{er} fixe le délai d'entrée en vigueur de la future loi et ne requiert aucune observation particulière.

En raison des changements importants notamment de nature informatique et technique qu'implique la nouvelle conservation ciblée par zones géographiques prévue à l'article 5bis nouveau de la Loi Telecom ainsi que l'interdiction de conservation généralisée et indifférenciée prévue aux articles 5 et 9 de la Loi Telecom, les auteurs du projet de loi entendent accorder un certain délai aux opérateurs et fournisseurs concernés par ces nouvelles dispositions pour prendre les mesures nécessaires pour s'y conformer. L'entrée en vigueur de ces trois dispositions s'effectuera ainsi le premier jour du douzième mois qui suit la publication du texte au Journal officiel du Grand-Duché de Luxembourg.

*

TEXTES COORDONNES

1. CODE DE PROCEDURE PENALE

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 **10bis 10ter, paragraphe 1^{er}**, 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 10ter, 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 1^{er} 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 paragraphes 1^{er} 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 **1^{er} (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 **324quater 324ter** 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 MODIFIEE DU 30 MAI 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

Art. 1^{er}. 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 **1^{er} 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 **1^{er} 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. 5bis. (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 événements 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 1^{er} 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 5ter. (1) Les données conservées au titre des articles 5, 5bis et 9 de la présente loi par les autorités compétentes au sens de l'article 1^{er}, paragraphe 1^{er}, de la loi du 1^{er} 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. 5quater. (1) La Commission nationale pour la protection des données **transmet public** 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 (5bis).
- (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.

(5bis) 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 1^{er}, 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 **1^{er} 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. 10ter. 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 10bis 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 1^{er} pendant le délai fixé à l'article 10bis, 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 1^{er} 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 1^{er} 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 1^{er} 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 1^{er} 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 1^{er} 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 1^{er} 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 1^{er} ainsi que les mesures de repérage visées au paragraphe 2, sauf à saisir sans désenparer 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 1^{er} 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.

*

FICHE FINANCIERE

Le projet de loi sous examen ne comporte pas de dispositions dont l'application est susceptible de grever le budget de l'Etat.

*

FICHE D’EVALUATION D’IMPACT

Coordonnées du projet

Intitulé du projet :	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
Ministère initiateur :	Ministère de la Justice
Auteur(s) :	Michèle SCHUMMER
Téléphone :	247-88562
Courriel :	michele.schummer@mj.etat.lu
Objectif(s) du projet :	Le présent projet de loi a pour objet d’adapter le dispositif légal national relatif à la rétention des données dans le secteur des communications électroniques aux exigences des derniers arrêts rendus par la Cour de Justice de l’Union européenne dans la matière, et notamment l’arrêt « Quadrature du Net » du 6 octobre 2020 (affaires C-511/18, C-512/18 et C-520/18 : La Quadrature du Net, French Data Network et Ordre des barreaux francophones et germanophone) ainsi que l’arrêt dans l’affaire C-140/20 « Commissioner of the Garda Síochána e. a. » du 5 avril 2022.
Autre(s) Ministère(s)/Organisme(s)/Commune(s)impliqué(e)(s) :	Ministère d’Etat, Autorités judiciaires
Date :	10/01/2023

Mieux légiférer

1. Partie(s) prenante(s) (organismes divers, citoyens, ...) consultée(s) : Oui Non
Si oui, laquelle/lesquelles : Ministère d’Etat, Ministère de la Sécurité intérieure, Autorités judiciaires, Opérateurs et fournisseurs de communications électroniques
Remarques/Observations : Néant
2. Destinataires du projet :

– Entreprises/Professions libérales :	Oui <input checked="" type="checkbox"/>	Non <input type="checkbox"/>
– Citoyens :	Oui <input checked="" type="checkbox"/>	Non <input type="checkbox"/>
– Administrations :	Oui <input checked="" type="checkbox"/>	Non <input type="checkbox"/>
3. Le principe « Think small first » est-il respecté ? Oui Non N.a.¹
(c.-à-d. des exemptions ou dérogations sont-elles prévues suivant la taille de l’entreprise et/ou son secteur d’activité ?)
Remarques/Observations :
4. Le projet est-il lisible et compréhensible pour le destinataire ? Oui Non
Existe-t-il un texte coordonné ou un guide pratique, mis à jour et publié d’une façon régulière ? Oui Non

¹ N.a. : non applicable.

Remarques/Observations : Un texte coordonné est joint au projet.

5. Le projet a-t-il saisi l'opportunité pour supprimer ou simplifier des régimes d'autorisation et de déclaration existants, ou pour améliorer la qualité des procédures ? Oui Non
 Remarques/Observations : Non applicable
6. Le projet contient-il une charge administrative² pour le(s) destinataire(s) ? (un coût imposé pour satisfaire à une obligation d'information émanant du projet ?) Oui Non
 Si oui, quel est le coût administratif³ approximatif total ? (nombre de destinataires x coût administratif par destinataire)
7. a) Le projet prend-il recours à un échange de données inter-administratif (national ou international) plutôt que de demander l'information au destinataire ? Oui Non N.a.
 Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il ?
- b) Le projet en question contient-il des dispositions spécifiques concernant la protection des personnes à l'égard du traitement des données à caractère personnel⁴ ? Oui Non N.a.
 Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il ?
 Données d'identification;
 Donn
8. Le projet prévoit-il :
 – une autorisation tacite en cas de non réponse de l'administration ? Oui Non N.a.
 – des délais de réponse à respecter par l'administration ? Oui Non N.a.
 – le principe que l'administration ne pourra demander des informations supplémentaires qu'une seule fois ? Oui Non N.a.
9. Y a-t-il une possibilité de regroupement de formalités et/ou de procédures (p.ex. prévues le cas échéant par un autre texte) ? Oui Non N.a.
 Si oui, laquelle :
10. En cas de transposition de directives communautaires, le principe « la directive, rien que la directive » est-il respecté ? Oui Non N.a.
 Sinon, pourquoi ?
11. Le projet contribue-t-il en général à une :
 a) simplification administrative, et/ou à une Oui Non
 b) amélioration de la qualité réglementaire ? Oui Non
 Remarques/Observations :

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

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

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

12. Des heures d'ouverture de guichet, favorables et adaptées aux besoins du/des destinataire(s), seront-elles introduites ? Oui Non N.a.
13. Y a-t-il une nécessité d'adapter un système informatique auprès de l'Etat (e-Government ou application back-office) ? Oui Non
Si oui, quel est le délai pour disposer du nouveau système ?
14. Y a-t-il un besoin en formation du personnel de l'administration concernée ? Oui Non N.a.
Si oui, lequel ?
Remarques/Observations :

Egalité des chances

15. Le projet est-il :
- principalement centré sur l'égalité des femmes et des hommes ? Oui Non
 - positif en matière d'égalité des femmes et des hommes ? Oui Non
Si oui, expliquez de quelle manière :
 - neutre en matière d'égalité des femmes et des hommes ? Oui Non
Si oui, expliquez pourquoi : Il s'agit de dispositions légales qui s'appliquent de la même façon et sans distinctions eu égard au sexe de la personne concernée par les procédures pénales en cause.
 - négatif en matière d'égalité des femmes et des hommes ? Oui Non
Si oui, expliquez de quelle manière :
16. Y a-t-il un impact financier différent sur les femmes et les hommes ? Oui Non N.a.
Si oui, expliquez de quelle manière :

Directive « services »

17. Le projet introduit-il une exigence relative à la liberté d'établissement soumise à évaluation⁵ ? Oui Non N.a.
Si oui, veuillez annexer le formulaire A, disponible au site Internet du Ministère de l'Economie et du Commerce extérieur :
www.eco.public.lu/attributions/dg2/d_consommation/d_march_int_rieur/Services/index.html
18. Le projet introduit-il une exigence relative à la libre prestation de services transfrontaliers⁶ ? Oui Non N.a.
Si oui, veuillez annexer le formulaire B, disponible au site Internet du Ministère de l'Economie et du Commerce extérieur :
www.eco.public.lu/attributions/dg2/d_consommation/d_march_int_rieur/Services/index.html

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

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

