Chambre des Députés
GRAND-DUCHÉ DE LUXEMBOURG

Dossier consolidé

Date de création : 22-05-2024

Projet de loi 8148

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

Date de dépôt : 08-02-2023
Date de l'avis du Conseil d'État : 23-01-2024
Auteur(s) : Madame Sam Tanson, Ministre de la Justice

Le document « 8148_7_Dossier_parlementaire » n'a pu être ajouté au dossier consolidé.

Liste des documents

8148/00

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

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

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

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

La décision écrite et motivée mentionne :

a) L'infraction qui fait l'objet de l'ordre ;

b) L'indication précise d'un ou de plusieurs des éléments suivants : la ou les personnes, les moyens de communication ou les lieux qui font l'objet de la conservation ;

c) La durée de conservation des données, qui ne peut excéder six mois. Ce délai peut être prolongé par écrit.

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

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

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

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

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

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

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

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

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

(2) Dans le cadre de l'enquête pour crime ou délit ou de l'instruction préparatoire et si les faits emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement, le procureur d'État ou le juge d'instruction peut, par une décision

motivée et écrite, en requérant au besoin le concours d'un opérateur de télécommunications ou d'un fournisseur d'un service de communications électroniques, procéder ou faire procéder sur la base de toutes données détenues par lui sur base de l'article 10*ter*, paragraphe 2, de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques à l'identification de l'utilisateur d'une adresse IP.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(3) La personne dont un moyen de télécommunication ou de communication électronique a fait l'objet de la mesure prévue au paragraphe 1er est informée de la mesure ordonnée au cours même

de l'instruction et en tout cas au plus tard dans les 12 mois qui courent à partir de la date de l'ordonnance. Toutefois ce délai de 12 mois ne s'applique pas lorsque la mesure a été ordonnée dans une instruction pour des faits qui se situent dans le cadre ou en relation avec une association ou une organisation criminelle au sens des articles 322 à 324*quater* du Code pénal, ou qui se situent dans le cadre ou en relation avec le terrorisme au sens des articles 135-1 à 135-6, 135-9 et 135-11 à 135-16 du Code pénal, ou au sens de l' article 10, alinéa 1 de la loi modifiée du 19 février 1973 concernant la vente de substances médicamenteuses et la lutte contre la toxicomanie.

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

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

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

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

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

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

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

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

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

« Art. 5. Données relatives au trafic

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

– ordonnés par les autorités judiciaires et par le comité ministériel du renseignement pour le Service de renseignement de l'Etat agissant dans le cadre des compétences leur attribuées par la loi pour sauvegarder la sécurité nationale, pour la lutte contre la criminalité grave et pour la prévention de menaces graves contre la sécurité publique, ou
– demandés par les organes compétents dans le but de régler des litiges notamment en matière d'interconnexion ou de facturation ».

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

(3) Les données relatives au trafic peuvent être traitées en vue de commercialiser des services de communications électroniques ou de fournir des services à valeur ajoutée dans la mesure et

pour la durée nécessaires à la fourniture ou à la commercialisation de ces services pour autant que le fournisseur d'un service de communications électroniques ou l'opérateur informe préalablement l'abonné ou l'utilisateur concerné des types de données relatives au trafic traitées, de la finalité et de la durée du traitement et que celui-ci ait donné son consentement, nonobstant son droit de s'opposer à tout moment à un tel traitement.

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

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

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

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

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

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

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

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

a) Les lieux où sont commis, de manière répétée, des crimes ou délits dont les faits emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement ;

b) Les lieux qui par leur configuration sont de nature à favoriser la commission des crimes ou délits dont les faits emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement ;

c) Les alentours et abords des infrastructures où sont organisés régulièrement des évènements d'envergure nationale ou internationale ;

d) Les lieux qui par leur nature rassemblent un grand nombre de personnes.

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

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

et indifférenciée des données relatives au trafic et à la localisation, sur l'ensemble du territoire.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

« (5*bis*) En outre, en cas de communication d'urgence, au sens de l'article 2, point 38°, de la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques, vers le numéro d'urgence unique européen 112 ainsi que vers les numéros d'urgence déterminés par l'Institut luxembourgeois de régulation, les informations relatives à la localisation de l'appelant obtenues à partir de l'appareil mobile, si elles sont disponibles, sont mises à disposition sans tarder

après l'établissement de la communication d'urgence au centre de réception des appels d'urgence le plus approprié, même lorsque l'appelant a désactivé la fonction de localisation. Ces informations sont à effacer après un délai de 24 heures au plus. »

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

*

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 1er, 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 1er 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 2014[1]

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 2016[2]

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 2020[4]

Par l'arrêt La Quadrature du Net du 6 octobre 2020 concernant trois affaires jointes[5] 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 article 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 2022[11]

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 2022[12]

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 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 indifférencie 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 PROPOSES 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 1er, 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 1er 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 2020[1] et du 5 avril 2022[2], 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 concernées[3]. 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 1er, point 1° 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 1er 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 1er, 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 1er, 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 1er, 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 1er, point 1° 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 10*ter* 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 10*bis* a été remplacée par celle de l'article 10*ter*, paragraphe 1er. L'article 1er, 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 10*ter*, 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 1er, point 1° du projet de loi, l'article 1er, 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 2014[6]. 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 reconnaitre 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 2015[8] 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 vœu 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 1er 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 media 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° 6763[3].

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° 2572/001[9], « *[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 1er, 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 1er, points 1° et 2° 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° – 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 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° – 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° propose de corriger la référence à l'article 3, paragraphe 1er, alinéa 2, en visant désormais, à la lumière du point 1°, 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 données[10] 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 2016[11], 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 1er de l'article 5 est partant supprimé et le paragraphe 2 devient le nouveau paragraphe 1er 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 1er 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 CJUE[12].

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 1er et 3 du projet de loi).

La modification du paragraphe 2, devenant le nouveau paragraphe 1er, 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 dérogatoires 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 5*bis*, paragraphe 1er, alinéa 1er, 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 5*bis*, paragraphe 1er, alinéa 1er, 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 5*bis*, paragraphe 1er, 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 1er, 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 5*bis*, 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 43*bis*, 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 5*bis*, 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 évènements 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 5*bis* 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 5*bis*, 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 procèdera 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 43*bis*, paragraphe 3, de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale.

Finalement, l'article 5*bis*, 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 1er, devenant le nouvel article 5*ter* 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 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale.

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 5*quater* 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 5*bis*, 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 10*ter* nouveau est scindé en deux paragraphes distinguant entre les données relatives à l'identité civile au paragraphe 1er, 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 infraction 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 10*bis* 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 10*bis* 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 10*bis* 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 10*ter* 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 un 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 duel 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 1er, 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 1er.

  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 1er 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 1er, 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 1er, 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'autrui*[20] ». 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 objectifs*[21] ».

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 rapport*[22] ».

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 limité 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 prévisible*[23] ». 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 (...) les 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 1er, point 1° du projet de loi et il est dès lors renvoyé aux explications fournies pour ladite disposition.

Ad Point 3° – 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 localisation[25].

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° 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° du nouvel article 7-2, paragraphe 1er, 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° 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 1er, 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 1er, 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 1er 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 5*bis* 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 ~~**10*bis***~~ **10*ter*, paragraphe 1er,** de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques à :

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

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

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

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

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

(4) Les dispositions ~~**du présent**~~ **des** paragraphe**s 1er à 3** sont à observer à peine de nullité.

~~**(2)**~~ **(5)** Chaque opérateur de télécommunications et chaque fournisseur d'un service de ~~**télécommunications**~~ **communications électroniques** communique les informations qui ont été demandées dans les meilleurs délais.

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

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

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

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

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

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

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

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

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

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

(3) La personne dont un moyen de télécommunication **ou de communication électronique** a fait l'objet de la mesure prévue au paragraphe **1er ~~(1)~~** est informée de la mesure ordonnée au cours même de l'instruction et en tout cas au plus tard dans les 12 mois qui courent à partir de la date de l'ordonnance. Toutefois ce délai de 12 mois ne s'applique pas lorsque la mesure a été ordonnée dans une instruction pour des faits qui se situent dans le cadre ou en relation avec une association ou une organisation criminelle au sens des articles 322 à **324*quater*** **~~324*ter*~~** du Code pénal, ou qui se situent dans le cadre ou en relation avec le terrorisme au sens des articles 135-1 à 135-6, 135-9 et 135-11 à 135-16 du Code pénal, ou au sens de l' article 10, alinéa 1 de la loi modifiée du 19 février 1973 concernant la vente de substances médicamenteuses et la lutte contre la toxicomanie.

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

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

*

2. LOI MODIFIEE DU 30 MAI 2005
concernant la protection de la vie privée dans le secteur des communications électroniques

Art. 1er. Champ d'application

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

Art. 2. Définitions

Aux fins de la présente loi on entend par:

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

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

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

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

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

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

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

(h) «réseau de communications électroniques»: les systèmes de transmission et, le cas échéant, les équipements de commutation ou de routage et les autres ressources qui permettent l'acheminement de signaux par câble, par voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques comprenant les réseaux satellitaires, les réseaux terrestres fixes (avec commutation de circuits ou de paquets, y compris l'Internet) et mobiles, les systèmes utilisant le réseau électrique, pour autant qu'ils servent à la transmission de signaux, les réseaux utilisés pour la radiodiffusion sonore et télévisuelle et les réseaux câblés de télévision, quel que soit le type d'information transmise;

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

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

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

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

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

Art. 3. Sécurité du traitement

(1) Le fournisseur de services prend les mesures techniques et d'organisation appropriées afin de garantir la sécurité de ses services, le cas échéant conjointement avec l'opérateur en ce qui concerne

la sécurité du réseau. En cas d'atteinte ou de risque d'atteinte grave à la sécurité du réseau ou des services, le fournisseur de services et le cas échéant l'opérateur prend les mesures appropriées pour y remédier, les frais étant à sa seule charge.

Sous réserve des dispositions générales **du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE** ~~**de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel**~~, les mesures visées ci-dessus, pour le moins:

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

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

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

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

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

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

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

La notification faite à l'abonné ou au particulier décrit au minimum la nature de la violation de données à caractère personnel et les points de contact auprès desquels des informations supplémentaires peuvent être obtenues et recommande des mesures à prendre pour atténuer les conséquences négatives possibles de la violation de données à caractère personnel. La notification faite à la Commission nationale pour la protection des données décrit en outre les conséquences de la violation de données à caractère personnel, et les mesures proposées ou prises par le fournisseur pour y remédier.

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

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

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

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

(5) Quiconque contrevient aux dispositions des paragraphes (1), (2) et (4) est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

Art. 4. Confidentialité des communications

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

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

(3) Le paragraphe (2):

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

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

(c) ne s'applique pas aux communications et aux données relatives au trafic y afférentes, effectuées à destination du numéro d'appel d'urgence unique européen 112 et des numéros d'urgence déterminés par l'Institut dans le seul but de permettre (a) la réécoute de messages lors de problèmes de compréhension ou d'ambiguïté entre l'appelant et l'appelé, (b) la documentation de fausses alertes, de menaces et d'appels abusifs et (c) la production de preuves lors de contestation sur le déroulement d'actions de secours.

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

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

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

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

Cette disposition ne fait pas obstacle à un stockage ou à un accès techniques visant exclusivement à effectuer la transmission d'une communication par la voie d'un réseau de communications

électroniques, ou strictement nécessaires au fournisseur pour la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur.

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

Art. 5. Données relatives au trafic

~~(1) (a) *(Loi du 24 juillet 2010)* « Pour les besoins de la recherche, de la constatation et de la poursuite d'infractions pénales qui emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement, et dans le seul but de permettre, en tant que de besoin, la mise à disposition des autorités judiciaires d'informations, tout fournisseur de services ou opérateur qui traite ou génère dans le cadre de la fourniture de services des données relatives au trafic est tenu de conserver ces données pendant une période de six mois à compter de la date de la communication. L'obligation de conserver inclut la conservation des données relatives aux appels téléphoniques infructueux lorsque ces données sont générées ou traitées et stockées (en ce qui concerne les données de la téléphonie) ou journalisées (en ce qui concerne les données de l'internet) dans le cadre de la fourniture des services de communications concernés. Un règlement grand-ducal détermine les catégories de données relatives au trafic susceptibles de pouvoir servir à la recherche, à la constatation et à la poursuite d'infractions visées ci-dessus. Ce règlement peut également déterminer les formes et les modalités suivant lesquelles les données visées sont à mettre à la disposition des autorités judiciaires ».~~

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

~~(2)~~ (1) Tout fournisseur de services **de communications électroniques** ou opérateur qui traite des données relatives au trafic concernant les abonnés et les utilisateurs, est tenu de prendre toutes les dispositions nécessaires pour que de telles données soient **effacées ou rendues anonymes ~~conservées pendant la période prévue sub (1) (a) de manière telle qu'il est impossible à quiconque d'accéder à ces données~~** dès lors qu'elles ne sont plus nécessaires à la transmission d'une communication ou aux traitements prévus par les dispositions **des paragraphes 2 et 3 ~~sub (3) et (4)~~**, à l'exception des accès qui sont:

– ordonnés par les autorités judiciaires **et par le comité ministériel du renseignement pour le Service de renseignement de l'Etat** agissant dans le cadre des compétences leur attribuées par la loi **~~et celles compétentes en vertu des articles 88-1 à 88-4 du Code d'instruction criminelle~~** pour sauvegarder **la sécurité nationale, pour la lutte contre la criminalité grave ~~la sûreté de l'Etat, la défense,~~ et pour la prévention de menaces graves contre** la sécurité publique **~~et pour la prévention, la recherche, la constatation et la poursuite des infractions pénales visées au paragraphe (1) (a)~~**, ou
– demandés par les organes compétents dans le but de régler des litiges notamment en matière d'interconnexion ou de facturation ».

~~(3)~~ (2) Les données relatives au trafic qui sont nécessaires en vue d'établir les factures des abonnés et aux fins des paiements d'interconnexion peuvent être traitées. Un tel traitement n'est possible que jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement et ne peut en tout état de cause dépasser 6 mois lorsque la facture a été payée et n'a pas fait l'objet de litige ou de contestation.

~~(4)~~ (3) Les données relatives au trafic peuvent être traitées en vue de commercialiser des services de communications électroniques ou de fournir des services à valeur ajoutée dans la mesure et pour la durée nécessaires à la fourniture ou à la commercialisation de ces services pour autant que le fournisseur d'un service de communications électroniques ou l'opérateur informe préalablement l'abonné ou l'utilisateur concerné des types de données relatives au trafic traitées, de la finalité et de la durée du

traitement et que celui-ci ait donné son consentement, nonobstant son droit de s'opposer à tout moment à un tel traitement.

~~(5)~~ **(4)** Le traitement des données relatives au trafic effectué dans le cas des activités visées aux paragraphes **1er à 3** ~~(1) à (4)~~ est restreint aux personnes agissant sous l'autorité du fournisseur de services ou de l'opérateur qui sont chargés d'assurer la facturation ou la gestion du trafic, répondre aux demandes de clientèle, détecter les fraudes, commercialiser les services de communications électroniques ou fournir un service à valeur ajoutée. Le traitement doit se limiter à ce qui est nécessaire à de telles activités.

~~(6)~~ **(5)** Quiconque contrevient aux dispositions des paragraphes **1er à 4** ~~(1) à (5)~~ du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

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

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

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

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

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

a) Les lieux où sont commis, de manière répétée, des crimes ou délits dont les faits emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement ;

b) Les lieux qui par leur configuration sont de nature à favoriser la commission des crimes ou délits dont les faits emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement ;

c) Les alentours et abords des infrastructures où sont organisés régulièrement des évènements d'envergure nationale ou internationale ;

d) Les lieux qui par leur nature rassemblent un grand nombre de personnes.

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

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

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

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

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

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

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

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

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

Art. ~~5-1~~ 5*ter*. (1) Les données conservées au titre des articles 5**, 5*bis*** et 9 **de la présente loi par les autorités compétentes au sens de l'article 1er, paragraphe 1er, de la loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale** sont soumises aux exigences prévues **à l'article 28 ~~aux articles 22 et 23~~** de **~~la~~ cette même** loi **~~modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.~~**

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

Art. ~~5-2.~~ 5*quater*. (1) La Commission nationale pour la protection des données **~~transmet~~ publie** annuellement **~~à la Commission de l'Union européenne~~** des statistiques sur la conservation de données au titre des articles 5 et 9.

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

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

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

Art. 6. Facturation détaillée

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

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

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

(1) Dans les cas où la présentation de l'identification de la ligne appelante est offerte, le fournisseur du service permet à l'abonné et à l'utilisateur appelant d'empêcher, par un moyen simple et gratuit, la

présentation de l'identification de la ligne appelante et ce, appel par appel. L'abonné appelant dispose de cette possibilité de manière permanente pour chaque ligne.

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

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

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

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

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

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

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

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

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

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

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

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

(8) L'abonné appelé prétendant être victime d'appels à contenu malveillant ou dérangeant peut demander l'identification de la ligne appelante ou connectée, des appels répétés ou intempestifs, déclarés comme étant malveillants ou dérangeants, lesquels ont été effectués ou repérés sur base d'un même numéro d'appel ou d'un même raccordement. Un règlement grand-ducal fixera les modalités à respecter

par le fournisseur du service ou l'opérateur ainsi que par les abonnés prétendant être victime d'appels à contenu malveillant ou dérangeant. Il précisera également les caractéristiques d'un appel à contenu malveillant ou dérangeant et déterminera l'utilisation de l'identification de la ligne appelante même si sa présentation est empêchée.

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

Art. 8. Renvoi automatique d'appels

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

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

~~(1) (a) *(Loi du 24 juillet 2010)* « Pour les besoins de la recherche, de la constatation et de la poursuite d'infractions pénales qui emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement, et dans le seul but de permettre, en tant que de besoin, la mise à disposition des autorités judiciaires d'informations, tout fournisseur de services ou opérateur qui traite ou génère dans le cadre de la fourniture de services des données de localisation autres que des données relatives au trafic est tenu de conserver ces données pendant une période de six mois à compter de la date de la communication. L'obligation de conserver inclut la conservation des données relatives aux appels téléphoniques infructueux lorsque ces données sont générées ou traitées et stockées (en ce qui concerne les données de la téléphonie) ou journalisées (en ce qui concerne les données de l'internet) dans le cadre de la fourniture des services de communications concernés. Pour l'application du présent paragraphe, une seule information de localisation est requise par communication ou appel. Un règlement grand-ducal détermine les catégories de données de localisation autres que les données relatives au trafic susceptibles de pouvoir servir à la recherche, à la constatation et à la poursuite d'infractions visées ci-dessus. Ce règlement peut également déterminer les formes et les modalités suivant lesquelles les données visées sont à mettre à la disposition des autorités judiciaires ».~~

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

~~(2)~~ (1) Tout fournisseur de services **de communications électroniques** ou opérateur qui traite des données de localisation, autres que les données relatives au trafic, concernant les abonnés et les utilisateurs, est tenu de prendre toutes les dispositions nécessaires à ce que de telles données soient **effacées ou rendues anonymes dès lors qu'elles ne sont plus nécessaires à la transmission d'une communication ou aux traitements prévus par les dispositions des paragraphes 2 et 3, ~~conservées pendant la période prévue au paragraphe (1), (a) de manière telle qu'il est impossible à quiconque d'accéder à ces données~~**, à l'exception des accès qui sont ordonnés par les autorités judiciaires **et par le comité ministériel du renseignement pour le Service de renseignement de l'Etat** agissant dans le cadre des compétences leur attribuées par la loi **~~et celles compétentes en vertu des articles 88-1 à 88-4 du Code d'instruction criminelle~~** pour sauvegarder **la sécurité nationale, pour la lutte contre la criminalité grave ~~la sûreté de l'Etat, la défense,~~ et pour la prévention de menaces graves contre** la sécurité publique **~~et pour la prévention, la recherche, la constatation et la poursuite des infractions pénales visées au paragraphe (1) (a)~~**.

~~(3)~~ (2) Tout fournisseur de services **concernés** ou opérateur ne peut traiter des données de localisation autres que les données relatives au trafic et concernant les abonnés ou les utilisateurs que si celles-ci ont été rendues anonymes ou moyennant le consentement de l'abonné ou de l'utilisateur, dans la mesure

et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée et sous réserve des dispositions des paragraphes **1er, 3 et 4** ~~**(2), (4) et (5)**~~.

~~**(4)**~~ **(3)** Le fournisseur ~~**du service**~~ **de services concernés** et le cas échéant l'opérateur informe préalablement l'abonné ou l'utilisateur sur les types de données de localisation traitées, autres que les données relatives au trafic, sur la ou les finalité(s) et la durée de ce traitement ainsi que sur la transmission de ces données à des tiers en vue de la fourniture du service à valeur ajoutée. L'abonné ou l'utilisateur a la possibilité de retirer à tout moment son consentement pour le traitement des données de localisation autres que les données relatives au trafic.

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

~~**(5)**~~ **(4)** Le traitement effectué des données de localisation, autres que les données relatives au trafic, dans le cas des activités visées aux paragraphes **1er à 3** ~~**(1) à (4)**~~ est restreint aux personnes agissant sous l'autorité du fournisseur de services ou de l'opérateur ou du tiers qui fournit le service à valeur ajoutée. Le traitement doit se limiter à ce qui est nécessaire à de telles activités.

~~**(6)**~~ **(5)** Quiconque contrevient aux dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement. La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

*

[articles 10 et 10bis inchangés]

*

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

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

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

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

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

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

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

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

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

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

(3) Quiconque contrevient aux dispositions du présent article est puni d'un emprisonnement de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement.

La juridiction saisie peut prononcer la cessation du traitement contraire aux dispositions du présent article sous peine d'astreinte dont le maximum est fixé par ladite juridiction.

*

[article 11 inchangé]

*

Art. 12. Commission nationale pour la protection des données

La Commission nationale pour la protection des données instituée par l'article ~~**32 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel**~~ **3 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données** est chargée d'assurer l'application des dispositions de la présente loi et de ses règlements d'exécution sans préjudice de l'application de l'article ~~**8 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel**~~ **5 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données**.

*

[articles 12bis à 16 inchangés]

*

3. LOI MODIFIEE DU 5 JUILLET 2016
portant réorganisation du Service de renseignement de l'Etat

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

(1) [écoutes]

(2) Sous réserve de respecter les principes de proportionnalité et de subsidiarité, le SRE est autorisé à procéder au repérage des données relatives au trafic, **y** compris l'identification des correspondants et de toutes les formes de communications ou à la localisation de l'origine ou de la destination de ces communications, en requérant au besoin le concours technique de l'opérateur de télécommunications et/ou du fournisseur d'un service de ~~**télécommunications**~~ **communications électroniques**.

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

Toute personne qui, du chef de sa fonction, a connaissance d'une des mesures prises en exécution du présent article ou y prête son concours, est tenue de garder le secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

*

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 ☒ Non ☐
   – Citoyens : Oui ☒ Non ☐
   – Administrations : Oui ☒ Non ☐

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

4. Le projet est-il lisible et compréhensible pour le destinataire ? Oui ☒ Non ☐
   Existe-t-il un texte coordonné ou un guide pratique, mis à jour et publié d'une façon régulière ? Oui ☐ Non ☒

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 administrative[2] pour le(s) destinataire(s) ? (un coût imposé pour satisfaire à une obligation d'information émanant du projet ?) Oui ☐ Non ☒

   Si oui, quel est le coût administratif[3] approximatif total ? (nombre de destinataires x coût administratif par destinataire)

7. a) Le projet prend-il recours à un échange de données inter-administratif (national ou international) plutôt que de demander l'information au destinataire ? Oui ☐ Non ☐ N.a. ☒

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

   b) Le projet en question contient-il des dispositions spécifiques concernant la protection des personnes à l'égard du traitement des données à caractère personnel[4] ? Oui ☒ Non ☐ N.a. ☐

   Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il ? Donnnées 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 évaluation[5] ? Oui ☐ Non ☒ N.a. ☐
Si oui, veuillez annexer le formulaire A, disponible au site Internet du Ministère de l'Economie et du Commerce extérieur :
www.eco.public.lu/attributions/dg2/d_consommation/d_march___int__rieur/Services/index.html

18. Le projet introduit-il une exigence relative à la libre prestation de services transfrontaliers[6] ? Oui ☐ Non ☒ N.a. ☐
Si oui, veuillez annexer le formulaire B, disponible au site Internet du Ministère de l'Economie et du Commerce extérieur :
www.eco.public.lu/attributions/dg2/d_consommation/d_march___int__rieur/Services/index.html

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

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

Impression: CTIE – Division Imprimés et Fournitures de bureau

8148/04

N° 8148[4]

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 électroniques ; et

3° de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat

* * *

AVIS DU TRIBUNAL D'ARRONDISSEMENT DE LUXEMBOURG

Dans un souci de lisibilité, seuls les articles et paragraphes du texte du projet de loi, pour lesquels il semble opportun de relever des points paraissant importants, ont été commentés.

Article 3

Le fait que l'action publique ne peut être mise en mouvement que par le seul Procureur d'État, trouve l'appui du Tribunal d'arrondissement, étant donné que, dans le cas contraire, l'activité gouvernementale risquerait, le cas échéant, d'être entravée, plus ou moins régulièrement.

Les droits des personnes lésées et des associations visées à l'article 3-1 du Code de procédure pénale restent, par ailleurs, intacts, étant donné que ces parties peuvent toujours porter plainte, de sorte à entraîner un examen par le Procurer d'État.

Articles 4, 5, 6 et 7

Ces articles prévoient, que, hormis le cas des crimes et des délits flagrants, le juge d'instruction, avant de décerner un mandat d'amener et d'arrêt, doit demander « l'autorisation préalable de la Chambre des Députés ». Le procureur général d'État soumettra la demande, accompagnée « d'un relevé des faits et indices et des qualifications possibles » à la Chambre des Députés.

Il faudrait préciser si l'adjectif « flagrants » s'applique aux « crimes et délits » ou uniquement aux « délits ».

C'est ici que se pose la question du respect de la séparation des pouvoirs. Le juge d'instruction, saisi d'une instruction, **« devra »** demander l'autorisation **« préalable »** de la Chambre des Députés avant d'émettre un mandat d'amener et d'arrêt. Cette demande sera accompagnée d'un relevé des faits, des indices et des qualifications possibles, ce qui signifie que la Chambre des Députés aura le droit d'agir, dans un premier temps, en lieu et place d'une juridiction, en décidant, sur base d'un dossier, s'il y a lieu, ou non, de poursuivre soit en donnant l'autorisation soit en la refusant.

N'y a-t-il pas, en cas d'adoption de ce texte, un amalgame des pouvoirs exercés par le pouvoir judicaire et le pouvoir législatif, l'un interférant dans les prérogatives de l'autre et devant donner son autorisation pour que l'autre puisse continuer à exercer son pouvoir ?

Prévoir ici l'intervention de la Chambre des Députés, en lui attribuant le pouvoir d'arrêter les poursuites pénales, fait en sorte qu'une décision soit prise dans un dossier pénal, sans aucune possibilité

de recours. Normalement, le Code de procédure pénale permet l'exercice des voies de recours par les parties concernées contre les décisions de la Chambre du conseil.

Le présent texte prévoit que « lorsque la Chambre des Députés ne donne pas son autorisation préalable, elle transmet sa réponse, accompagnée des pièces lui transmises, au procureur général d'État qui la transmet au juge d'instruction. ». L'alinéa 2 stipule ensuite que le juge d'instruction « communique le dossier au procureur d'État ». Le texte ne mentionne aucune voie de recours contre cette décision de la Chambre des Députés.

L'absence d'un tel recours soulève, entre autres, de façon générale la question, pourquoi, si une personne, visée par l'article 1 du présent projet de loi, fait l'objet d'une instruction concernant une infraction pénale commise dans l'exercice de ses fonctions, ne serait pas poursuivie et jugée selon les mêmes formes que tous les autres justiciables ?

Les autres alinéas du nouveau texte n'appellent pas de commentaire particulier.

Impression: CTIE – Division Imprimés et Fournitures de bureau

8148/02

N° 8148²

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 électroniques ; et

3° de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat

* * *

AVIS DU PARQUET GENERAL

(13.3.2023)

A titre liminaire, il importe de relever l'importance primordiale pour la poursuite d'infractions graves, de la mise à disposition des autorités judiciaires de données de télécommunications, notamment à travers le recueil, auprès des opérateurs de télécommunications et des fournisseurs de services de communications électroniques, de données relatives au trafic et à la localisation, essentiellement pour combattre une criminalité grave et/ou organisée.

Ainsi l'expérience a montré que dans nombre d'affaires caractérisées par la gravité particulière des faits à leur base – ayant causé d'importants troubles à l'ordre public et en conséquence un sentiment d'insécurité croissant dans l'opinion publique – le repérage et la géolocalisation constituent des outils essentiels à la disposition des autorités chargées de la poursuite de ces infractions pénales graves, en contribuant en large partie, voire parfois exclusivement à résoudre ces affaires d'envergure.

En effet, les auteurs de tels faits graves s'assurent généralement, en ayant recours à une préparation minutieuse de leur méfait et en se dotant de moyens souvent considérables, que les méthodes d'investigation traditionnelles à la disposition des autorités poursuivantes soient rapidement mises en échec, afin de tenter de se mettre à l'abri des poursuites.

Le repérage téléphonique est régulièrement un facteur clé dans l'identification et la poursuite d'individus attribués à la criminalité organisée ou d'auteurs d'infractions graves.

Renvoyons à titre d'exemple au cas des membres d'une association qui se déplaçaient de la région parisienne jusqu'au Luxembourg pour y commettre une série de vols qualifiés, notamment des vols à main armée commis avec violences dans des maisons habitées.

Dans cette affaire, les repérages téléphoniques ont constitué un élément déterminant dans l'identification et la poursuite des auteurs de ces faits.

Ainsi, l'exploitation des données relatives au trafic et à la localisation a permis de démontrer des déplacements des auteurs de la région parisienne vers la région frontalière franco luxembourgeoise dans les heures précédant les infractions commises au Luxembourg, suivis d'une absence inhabituelle d'activités sur ces lignes téléphoniques pendant les périodes d'infractions correspondantes ainsi qu'un retour en région parisienne par la suite.

Citons aussi à titre d'exemple l'affaire de la disparition d'une jeune femme à Luxembourg-Ville, dont le corps calciné a été retrouvé quelques heures après sa disparition dans un véhicule carbonisé, abandonné sur un chemin rural.

Le repérage des télécommunications et la géolocalisation ont finalement permis d'établir la culpabilité de l'auteur des faits dont fût victime la jeune femme, lequel n'aurait très probablement pas manqué d'échapper à sa condamnation, eu égard à la parcimonie des autres indices qui existaient à sa charge.

Ainsi, les informations tirées de la téléphonie se sont révélées capitales, étant donné qu'elles ont finalement permis de reconstituer le déroulement de la journée de l'auteur des faits, entre un point temporel antérieur à la disparition de la victime et le moment de la découverte du corps de cette dernière, y compris les déplacements effectués par l'auteur le soir des faits ayant précédé cette disparition.

Ces données ont ainsi permis d'infirmer nombre de déclarations mensongères de l'auteur des faits et ont, en large partie, contribué à réunir un faisceau d'indices à charge du prévenu ayant conduit à sa condamnation définitive du chef d'assassinat.

Ces exemples démontrent que le recours aux données relatives au trafic et à la localisation des communications constituent des moyens efficaces, souvent primordiaux dans la lutte contre la criminalité grave et/ou organisée, qui constitue une menace grave, actuelle et réelle pour les citoyens.

Il s'agit dans un nombre important de cas d'une condition déterminante du succès des enquêtes menées et il n'existe pas de méthodes d'enquête alternatives qui pourraient s'y substituer de manière efficace.

Le cas de figure dans lequel les enquêteurs se trouvent confrontés à une situation où la seule piste d'enquête exploitable consiste dans la détermination des lignes téléphoniques actives sur les lieux de l'infraction au moment des faits afin de pouvoir identifier l'auteur d'une infraction grave n'est pas un cas d'école.

Tel a par exemple été le cas pour une série de vols à main armée commis dans des stations de service.

Ni les déclarations des témoins entendus, ni l'exploitation des traces génétiques relevées sur les lieux des différentes infractions, ni l'exploitation des images provenant des systèmes de vidéo surveillance des stations visées, ni plus une observation systématique des lieux, n'ont permis de faire avancer l'enquête.

Le recueil des données téléphoniques demeurait ainsi seul moyen à la disposition des enquêteurs pour tenter l'identification de l'auteur par le biais de la détermination d'un dénominateur commun reliant les différents faits commis, en identifiant un même numéro de téléphone relié aux pylônes de transmission couvrant les différents lieux d'infraction au moment des faits respectifs.

D'aucuns argumenteront que dans un tel cas de figure, les autorités poursuivantes scruteraient les données téléphoniques au peigne fin au point que les citoyens irréprochables verraient leur vie privée épinglée. C'est méconnaître la méthode de travail en matière d'identification des auteurs d'infractions. Les enquêteurs procèdent à une sorte de filtrage des données et ne s'intéressent qu'aux seules données faisant entrevoir un lien entre le titulaire d'une ligne téléphonique et l'affaire pénale qu'ils essaient de résoudre, par exemple en raison d'un lien personnel existant entre le titulaire d'une ligne téléphonique repérée sur les lieux de l'infraction et la victime ou en raison de la connexion d'un même numéro de téléphone aux pylônes de transmission couvrant différents lieux d'infractions séparés dans l'espace, constituant ainsi un dénominateur commun permettant le cas échéant l'identification de l'auteur de ces infractions.

La liste d'importantes affaires criminelles résolues grâce au repérage téléphonique ou au recueil de données conservées par les opérateurs de télécommunications et les fournisseurs de services de communications électroniques est longue et le recours à ces outils se fait en pratique dans des affaires criminelles et correctionnelles graves, telles que des affaires de meurtres, d'incendies criminels, de braquages, de vols à l'aide de violences, d'extorsions, de prises d'otages, d'attaques sur des distributeurs automatiques de billets de banque à l'aide d'explosifs ou encore de trafics de stupéfiants organisés.

L'importance primordiale pour les autorités judiciaires de disposer également à l'avenir de ces outils, découle aussi du constat que la criminalité organisée, qui a souvent un caractère transnational, ne cesse de prospérer à l'ère de la mondialisation où les frontières se sont ouvertes et où l'information se propage de manière quasiment instantanée autour du monde à l'aide des moyens de communication modernes.

En 2019, les recettes d'origine criminelle sur les principaux marchés criminels représentaient 1 % du PIB de l'UE, soit 139 milliards d'euros d'après les informations publiées sur site web officiel du Conseil de l'UE et du Conseil européen[1].

Le constat d'une menace croissante résultant des activités d'organisations criminelles qui ont de plus en plus recours aux nouvelles technologies et saisissent toutes les occasions pour développer leurs activités illégales, a amené la Commission européenne à définir une stratégie visant à stimuler la coopération dans l'ensemble de l'UE et à mieux exploiter les outils numériques dans le cadre des enquêtes.

La stratégie définie vise notamment à soutenir des enquêtes plus efficaces afin de désorganiser les structures de la criminalité organisée et de cibler des formes de criminalité spécifiques et à adapter les services répressifs et l'appareil judiciaire à l'ère numérique.

Dans un communiqué de presse de la Commission, on peut ainsi lire que « *80 % des infractions possédant une composante numérique, les services répressifs et l'appareil judiciaire ont besoin d'un accès rapide aux preuves et aux indices numériques. Ils doivent également utiliser les nouvelles technologies et être dotés d'outils et de compétences leur permettant de suivre les nouveaux modes opératoires des criminels. La Commission analysera et définira les approches envisageables en matière de conservation des données et proposera une voie à suivre pour aborder la question d'un accès légal et ciblé aux informations cryptées dans Je cadre d'enquêtes et de poursuites pénales, tout en protégeant la sécurité et la confidentialité des communications.* »[2]

Il va sans dire que le phénomène de la criminalité grave à caractère transnational touche indiscutablement tous les pays à l'ère de la mondialisation mais on peut admettre que pour des raisons géographiques évidentes, le Luxembourg risque d'y être particulièrement exposé, d'un côté en raison du fait qu'il a des frontières communes avec trois pays voisins et d'un autre côté en raison de sa position centrale en Europe, de sorte qu'il est une cible convoitée par des malfrats qui se déplacent au Luxembourg pour y commettre leurs méfaits avant de prendre rapidement la fuite en franchissant la frontière à un moment rapproché des faits.

Le projet de loi examiné entend mettre en conformité la législation nationale en matière de rétention des données avec les principes posés par la jurisprudence de la Cour de Justice de l'Union Européenne en matière de traitement des données à caractère personnel dans le secteur des communications électroniques.

Ces principes dégagés par la Cour de Justice de l'Union Européenne dans une série d'arrêts (Digital Rights lreland Ltd contre Minister for Communications, Marine and Natural Resources e.a. et Kärntner Landesregierung e.a. Arrêt Tele2 et Watson Quadrature du Net et Commissioner of An Garda Síochána e.a.) peuvent être synthétisés de la manière suivante :

Une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation est clairement exclue. Seule une menace grave pour la sécurité nationale, qui s'avère réelle et actuelle ou prévisible, justifie 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. En effet, seul ce cas de figure justifie l'injonction aux fournisseurs de services de communications électroniques de conserver de manière généralisée et indifférenciée des données relatives au trafic et à la localisation.

L'injonction aux fournisseurs de services de communications électroniques de conserver de manière généralisée et indifférenciée des données relatives au trafic et à la localisation 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 de l'une des situations de menace envisagées ainsi que le respect des conditions et des garanties prévues.

Une législation nationale imposant la conservation de données relatives au trafic et des données de localisation est également admise pour les besoins de la recherche, de la constatation et de la poursuite d'infractions présentant un degré de gravité suffisant, à condition toutefois qu'il s'agisse d'une conservation ciblée.

En effet, le juge de l'Union rappelle qu'un tel objectif d'intérêt général tel que la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme, aussi fondamental qu'il

---

1 https://www.consilium.europa.eu/fr/policies/eu-fight-against-crime/

2 https://ec.europa.eu/commission/presscorner/detail/fr/ip_21_1662

soit, ne saurait à lui seul justifier qu'une réglementation nationale prévoie la conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation.

La jurisprudence européenne exige ainsi la nécessité de critères objectifs permettant de délimiter la conservation des données, l'accès des autorités nationales compétentes à ces données et leur utilisation ultérieure à des fins de prévention, de détection ou de poursuites pénales concernant des infractions pouvant être considérées comme suffisamment graves pour justifier une telle ingérence.

La conservation des données pendant une période d'au moins six mois sans que soit opérée une quelconque distinction entre les catégories de données en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées, est exclue.

Aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, est admise la conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées, susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable.

Le juge de l'Union relève qu'il ne saurait être exclu que d'autres critères, objectifs et non discriminatoires, puissent entrer en ligne de compte afin d'assurer que la portée d'une conservation ciblée soit limitée au strict nécessaire.

La 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 concernées ou au moyen d'un critère géographique, voire d'autres critères objectifs, doit par ailleurs 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.

La jurisprudence européenne ne s'oppose pas non plus à une mesure législative permettant le recours à une conservation rapide (« quick freeze ») des données dont disposent les fournisseurs de services, dès lors que se présentent des situations dans lesquelles survient la nécessité de conserver lesdites données au-delà des délais légaux de conservation des données aux fins de l'élucidation d'infractions pénales graves ou d'atteintes à la sécurité nationale, lorsque ces infractions ou atteintes ont déjà été constatées ou lorsque leur existence peut être raisonnablement soupçonnée.

La conservation rapide (« quick freeze ») des données relatives au trafic et des données de localisation ne peut intervenir, pour une durée déterminée, qu'en vertu d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif. Seule la lutte contre la criminalité grave et la sauvegarde de la sécurité nationale sont de nature à justifier une telle conservation, à la condition que cette mesure ainsi que l'accès aux données conservées respectent les limites du strict nécessaire. Plus précisément, les données ainsi conservées doivent contribuer à la poursuite d'infractions graves sur base d'éléments objectifs et non discriminatoires.

Une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une communication, pour une période temporellement limitée au strict nécessaire, ainsi que des données relatives à l'identité civile des utilisateurs de communications électroniques, est admise.

La CJUE a relevé que l'ingérence sous forme de mesures législatives en matière de conservation de données doit avoir un caractère proportionné par rapport à l'objectif poursuivi. Elle a fait le choix de garantir un niveau élevé de protection des données à caractère personnel et de la vie privée pour les services de communications électroniques.

Le juge de l'Union semble par ailleurs considérer qu'un tel choix n'a qu'une répercussion modérée sur l'efficacité des poursuites pénales, en admettant que « *l'efficacité de poursuites pénales dépend généralement non pas d'un seul instrument d'enquête, mais de tous les instruments d'enquête dont disposent les autorités nationales compétentes à ces fins*[3] »

Or, tel que cela a été exposé ci-dessus, la pratique a révélé qu'au contraire, la conservation des données relatives au trafic et des données de localisation et l'accès des autorités judiciaires à ces

3 Point 60 de l'arrêt de la Cour de Justice de l'Union Européenne du 5 avril 2022 dans l'affaire G.D. contre Commissioner of An Garda Síochána e.a.

données a, dans bon nombre d'affaires, été l'unique moyen de retrouver le ou les auteur(s) d'infractions pénales graves.

*

COMMENTAIRE DES ARTICLES

Article 1er 1°

Cet article propose d'introduire un nouvel article 24-3 dans le Code de procédure pénale qui permet au procureur d'Etat d'ordonner, pour les besoins de la recherche, de la constatation et de la poursuite d'infractions pénales, la conservation rapide auprès des opérateurs de télécommunications et des fournisseurs de services de communications électroniques, de données relatives au trafic et à la localisation.

Le but recherché par cette disposition consiste dans la conservation rapide des données aux fins de l'élucidation d'infractions pénales graves, lorsque ces infractions ont déjà été constatées ou lorsque leur existence peut être raisonnablement soupçonnée.

L'article 24-3 du Code de procédure pénale introduit une conservation ciblée des données générées postérieurement à la commission d'une infraction et interviendra donc pour le futur.

On pourrait soulever une certaine incohérence de la mesure étant donné qu'elle instaure une conservation de données dans le futur, les auteurs d'infractions n'étant évidemment pas connus d'avance, pas plus que le lieu et la date de l'infraction. Il s'agira partant nécessairement d'une conservation de données se rapportant à une infraction qui a été commise ou à des personnes susceptibles d'être impliquées d'une manière ou d'une autre dans la commission de cette infraction (auteurs, victimes).

Or, il est à noter que la conservation des données pour le futur est d'une utilité toute relative en matière de poursuites d'infractions qui ont été commises, alors que les besoins de l'enquête nécessitent en général un retour en arrière, plus précisément, une exploitation des données se rapportant au jour même de la commission de l'infraction, respectivement aux heures, voire aux jours précédant la commission de l'infraction, afin de pouvoir éventuellement identifier un auteur, respectivement afin de pouvoir confirmer ou infirmer l'implication d'une personne dans la commission des faits et afin de pouvoir éventuellement retracer des préparatifs préalables à la commission de l'infraction.

Une conservation des données futures n'est certes pas dépourvue d'intérêt dans certaines hypothèses mais il convient de noter qu'elle n'aura son importance que dans un nombre limité de cas de figure, par exemple lorsqu'il s'agira de localiser la victime d'un enlèvement en cours ou de repérer ou de localiser un téléphone portable qui constitue l'objet d'une infraction ou qui a servi à commettre une infraction.

La conservation rapide intervient sur décision du procureur d'Etat. Il est au stade de l'enquête préliminaire l'autorité compétente et il est soumis à un contrôle juridictionnel effectif, notamment en application des dispositions de l'article 48-2 du Code de procédure pénale.

Afin de suffire aux exigences du juge de l'Union, l'article proposé limite la possibilité de recours à la conservation rapide à la seule recherche, à la constatation et à la poursuite des crimes et de certains délits, à savoir ceux qui sont punis d'un emprisonnement dont le maximum est égal ou supérieur à un an.

Le seuil de peine choisi devra mettre en équilibre deux impératifs difficilement conciliables, à savoir l'efficacité d'un système de poursuites d'un côté, et la protection des données de l'autre.

Plus ce seuil est élevé, moins un système des poursuites n'est efficace.

Or, dans ce contexte, il convient de rappeler que l'efficacité du système des poursuites a une conséquence directe sur l'évolution de la criminalité. En effet, moins un système répressif est efficace, plus un milieu criminel a tendance à prospérer. Une croissance de la criminalité aura de son côté un impact direct sur la sécurité publique, une augmentation des atteintes aux personnes et aux biens en étant la conséquence inéluctable.

La question de la proportionnalité d'une limitation de la confidentialité des communications résultant d'une conservation des données devra donc forcément s'analyser sous ce point de vue.

Est-il utile de rendre largement prioritaire la protection des données par rapport à l'efficacité des mesures de protection de l'ordre public – ou non – à une époque où sont nombreux ceux qui renoncent

de leur plein gré à une protection de leur vie privée en publiant spontanément toutes sortes de données personnelles sur des réseaux sociaux et où, en même temps, une criminalité grave ne cesse de prospérer ?

L'article proposé retient le même seuil de peine que celui figurant à l'article 67-1 du Code de procédure pénale, dans sa teneur actuelle. Ce choix semble logique dans la mesure où l'article 24-3 du Code de procédure pénale est censé permettre la conservation rapide de données auxquelles les autorités judiciaires ne pourront accéder par la suite qu'en vertu d'une ordonnance du juge d'instruction rendue en application des dispositions de l'article 67-1 du Code de procédure pénale.

La décision du procureur d'Etat d'ordonner pour les besoins de la recherche, de la constatation et de la poursuite d'infractions pénales, la conservation rapide, auprès des opérateurs de télécommunications et des fournisseurs de services de communications électroniques, de données relatives au trafic et à la localisation doit répondre à certains critères de forme et de fond.

Ces critères permettront de répondre aux exigences de la jurisprudence de la CJUE, qui retient que la conservation ciblée de données ne peut intervenir que sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique.

La décision du procureur d'Etat devra intervenir sous forme d'un écrit, dont le contenu devra mentionner l'infraction poursuivie, en vertu de laquelle la décision intervient. Le terme d'infraction utilisé semble engendrer la nécessité de libeller dans le corps de la décision le fait concret qui est poursuivi ou du moins la qualification juridique que ce dernier est susceptible de revêtir.

La décision devra en outre désigner ou bien la personne concernée par la mesure, ou bien les moyens de communication visées ou bien les lieux concernés. Ces précisions permettront d'apprécier que la conservation ciblée aura lieu en vue de la poursuite d'infractions graves sur base d'éléments objectifs et non discriminatoires.

En cas d'urgence, le procureur d'Etat pourra ordonner oralement la conservation rapide. La décision devra être formalisée par un écrit, répondant aux exigences exposées ci-dessus, dans les plus brefs délais.

La durée de conservation des données est limitée à une durée de 6 mois. L'article proposé prévoit que ce délai peut être prolongé, sans autres précisions.

Dans un souci de sécurité juridique, il conviendrait le cas échéant de préciser les conditions de forme et de fond que devra remplir cette décision de prolongation et de préciser la durée maximale de cette prolongation. Le principe du parallélisme des formes implique qu'une décision du procureur d'Etat ordonnant la prolongation de la mesure de conservation devrait se présenter sous une forme écrite, comportant une motivation suffisante afin de justifier que cette prolongation intervienne dans le respect des principes posés par le juge de l'Union et repris par les auteurs du projet de loi. Aussi conviendrait-il le cas échéant de préciser si le délai de conservation pourra être prolongé une seule fois ou plusieurs fois consécutives.

Il se pose par ailleurs la question de savoir quelle sera l'autorité compétente pour ordonner la prolongation du délai de conservation des données relatives au trafic et à la localisation dans l'hypothèse où le procureur d'Etat a ordonné une telle conservation et qu'il a par la suite saisi un juge d'instruction. Le procureur d'Etat étant dessaisi à partir de la saisine du juge d'instruction, il ne pourra plus ordonner une telle prolongation. Le juge d'instruction pourrait-il dans un pareil cas de figure ordonner la prolongation en question, en cas de besoin ?

L'article n'envisage pas cette hypothèse.

Dans ce contexte, il convient encore de relever qu'aucune disposition légale ne prévoit la possibilité pour un juge d'instruction d'ordonner la conservation ciblée pour le futur de données relatives au trafic et à la localisation[4].

---

4 L'article 48-25 du Code de procédure pénale prévoit uniquement la faculté pour le juge d'instruction de faire procéder à une conservation rapide et immédiate de données informatiques.

L'article 48-27 du Code de procédure pénale, tel que proposé, permet uniquement au juge d'instruction de faire procéder à l'identification d'un utilisateur ou de l'abonné d'un service de télécommunication, l'identification des services de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisées par elle et l'identification de l'utilisateur d'une adresse IP.

Une telle possibilité pourrait néanmoins s'avérer utile, par exemple dans un cas de figure où le magistrat instructeur est chargé d'une information du chef de faits constitutifs d'un enlèvement de mineur.

L'article proposé soumet les personnes appelées à avoir connaissance de cette mesure de conservation ciblée ou à y prêter leur concours à une obligation de secret dont la violation expose son auteur aux sanctions prévues par l'article 458 du Code pénal.

Cette obligation de secret et la sanction du non-respect de cette obligation s'impose eu égard aux impératifs de l'enquête pénale en cours et du respect de la présomption d'innocence et de la vie privée de la personne qui est le cas échéant nommément visée dans la décision de conservation rapide émanant du procureur d'Etat (et le cas échéant identifiable en tant que personne susceptible d'avoir participé à une infraction).

En effet, la fuite d'une information concernant une enquête en cours serait de nature à nuire à l'enquête et serait contraire à la présomption d'innocence dont bénéficie toute personne visée par des poursuites pénales.

L'article proposé prévoit encore que toute personne qui refuse de prêter son concours technique aux réquisitions visées dans l'article encourt une peine d'amende de 1.250 à 125.000 euros.

La nécessité de cette disposition découle du fait qu'un tiers qui refuserait d'obtempérer à la décision du procureur d'Etat pourrait mettre en échec cette décision et serait ainsi en mesure de nuire gravement à une enquête pénale en cours. Ce refus risquerait le cas échéant de favoriser la commission d'un nouveau crime ou d'un nouveau délit.

La sanction pénale du refus de prêter son concours technique à l'exécution de la décision du procureur d'Etat a partant tout son sens.

Etant donné qu'un tel refus pourrait potentiellement permettre la commission d'un nouveau crime ou d'un nouveau délit par un auteur qui n'a pas pu être identifié suite à ce refus, il se pose la question de savoir s'il ne convient pas de prévoir une aggravation de la peine qu'encourt le tiers qui refuse d'obtempérer dans un tel cas de figure, à l'instar de certaines dispositions similaires qui existent dans des législations étrangères[5].

Article 1er 2°

Cet article modifie l'article 48-27 du Code de procédure pénale.

L'article modifie la référence à l'article 10bis contenue dans l'article 48-27 actuel du Code de procédure pénale, en la remplaçant par la référence à l'article 10ter, en prévision de l'introduction de ce nouvel article 10ter dans la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

L'article proposé introduit également la possibilité pour le procureur d'Etat ou le juge d'instruction, de faire procéder, par décision écrite et motivée, à l'identification de l'utilisateur d'une adresse IP.

L'article limite cette possibilité d'identification aux enquêtes et instructions diligentées pour des faits constitutifs de crimes ou de délits punis d'un emprisonnement dont le maximum est égal ou supérieur à un an. Le seuil de peine choisi est identique à celui prévu à l'article 24-3 du Code de procédure pénale.

Les dispositions ayant trait à l'obligation de secret s'imposant aux personnes appelées à avoir connaissance de cette mesure ou à y prêter leur concours et la sanction du non-respect de cette obligation ainsi que celles relatives aux sanctions auxquelles s'expose un tiers qui refuserait d'obtempérer n'appellent pas d'observations particulières et il est renvoyé à ce qui a été exposé ci-dessus.

---

5 Par exemple l'article 434-15-2 du Code pénal français concernant le refus de remettre une convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit et qui dispose ce qui suit : (…) Si le refus est opposé alors que la remise ou la mise en œuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets, la peine est portée à cinq ans d'emprisonnement et à 450 000 € d'amende.

Article 1er 3°

Cet article modifie l'article 67-1 du Code de procédure pénale. L'article étend la possibilité d'un repérage au-delà des télécommunications en y ajoutant les communications électroniques, et en adaptant la terminologie employée à cette extension.

L'article proposé prévoit que toute personne qui refuse de prêter son concours technique aux réquisitions visées dans l'article encourt une peine d'amende de 100 à 5.000 euros.

Il se pose la question de savoir s'il n'était pas opportun d'aligner les dispositions pénales applicables en cas de refus d'une personne de prêter son concours technique aux réquisitions des autorités judiciaires, et de prévoir les mêmes taux pour les amendes encourues dans les différents cas de figure de refus d'obtempérer.

En effet, le refus d'un tiers d'obtempérer est dans tous les cas de figure de nature à mettre en échec la décision de l'autorité judiciaire compétente et de nuire ainsi gravement à une procédure pénale en cours et risque le cas échéant de favoriser la commission d'un nouveau crime ou délit.

Les autres dispositions de l'article n'appellent pas d'observations particulières.

Article 2 1°

L'article proposé modifie l'article 2 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques.

Cet article précise la notion de « consentement » et n'impose pas de remarque particulière.

Article 2 2°

Cet article qui modifie l'article 3 de la loi modifiée du 30 mai 2005 concernant la de la vie privée dans le secteur des communications électroniques ne suscite pas d'observations.

Article 2 3°

L'article proposé modifie l'article 5 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, afin de transposer en droit interne les principes posés par la jurisprudence de la CJUE, en matière de traitement des données à caractère personnel dans le secteur des communications électroniques.

Cet article transpose donc l'interdiction d'une conservation généralisée et indifférenciée des données relatives au trafic dans le domaine de la recherche, de la constatation et de la poursuite d'infractions pénales.

Il introduit la possibilité d'une conservation ciblée des données relatives au trafic dans le domaine de la recherche, de la constatation et de la poursuite d'infractions pénales.

Il est renvoyé aux développements précédents au sujet de l'importance capitale de la mise à disposition des autorités judiciaires de données téléphoniques, tant relatives au trafic que relatives à la localisation, pour la poursuite d'infractions pénales dans les conditions définies par la jurisprudence de la CJUE.

Tel qu'il a été relevé ci-dessus, la conservation des données de trafic et de localisation s'est régulièrement avérée être une condition déterminante pour le succès d'enquêtes pénales diligentées pour des faits graves dans le passé.

Si ces données devaient être perdues de manière substantielle, voire dans leur intégralité, l'efficacité du système de poursuites en pâtirait au point de réduire à néant la perspective de pouvoir identifier le ou les auteurs d'atteintes graves aux personnes et aux biens dans un nombre important d'affaires pénales.

Certains criminels bénéficieraient alors d'une sorte de garantie d'impunité prolongée dans le temps avec des risques de récidive démultipliés et toutes les conséquences qui s'en suivent pour la sécurité des citoyens.

Dans certains cas de figure concrets, la question de la proportionnalité risquerait alors de se poser dans un tout autre sens.

On serait alors amené à devoir se poser la question de savoir si la protection de la vie privée n'a pas été privilégiée au détriment de la protection de la vie tout court.

Article 2 4°

L'article proposé introduit l'article 5bis dans la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

Le choix du législateur pour concilier les deux objectifs difficilement compatibles – l'efficacité d'un système de poursuites d'un côté et la protection des données de l'autre – consiste à opter pour une conservation ciblée des données de télécommunication et de communications électroniques (relatives au trafic et à la localisation) à opérer, dans un but de lutte contre la criminalité grave et de la prévention de menaces graves contre la sécurité publique, limitée dans le temps, sur base d'un critère géographique.

L'article analysé précise les zones géographiques pour lesquelles les données devront être conservées, à savoir 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.

Il s'agira notamment des lieux où sont commis de manière répétée des faits emportant une peine criminelle ou une peine d'emprisonnement dont le maximum est égal ou supérieur à un an et des lieux, qui en raison de leur configuration, favorisent la commission de tels faits.

Le seuil de peine choisi pour mettre en équilibre les deux impératifs d'efficacité du système de poursuites et de la protection des données semble adapté et se situe dans la logique des seuils de peine prévues par les autres dispositions applicables en la matière.

Il s'agira également de lieux où ont régulièrement lieu des évènements d'envergure nationale ou internationale de même que ceux qui rassemblent par nature un grand nombre de personnes.

Le choix de ces endroits est adapté compte tenu du risque accru de commission d'infractions graves dans ces endroits qui en raison de leur localisation, de leur disposition ou de leur fréquentation constituent des lieux propices à la commission d'infractions. Les critères retenus pour déterminer ces zones étant par ailleurs objectifs et non-discriminatoires, la disposition textuelle suffit également aux exigences de la jurisprudence de la CJUE.

Les zones géographiques visées par une conservation ciblée seront le cas échéant modifiées en fonction de l'évolution des conditions ayant justifié leur sélection.

L'étendue du périmètre de chaque zone sera déterminée par arrêté grand-ducal sur proposition de la commission consultative au Haut-Commissariat à la protection nationale dont la création est prévue aux termes de paragraphe 4 de l'article 5bis.

La composition et les modalités de cette commission seront fixées par un règlement grand-ducal.

La sélection des zones concernées et la détermination, avec précision, de leur périmètre seront capitales pour assurer le maintien de l'efficacité du système de poursuites qui dépendra dans une très large mesure des choix faits à ce niveau.

L'article proposé retient que les opérateurs seront tenus de conserver les données de trafic pour toutes les communications ou appels effectués à partir d'une zone géographique sélectionnée ou vers une telle zone et lorsque l'utilisateur final se déplace pendant une communication électronique, l'opérateur devra conserver les données pour autant que l'utilisateur final se trouve à un moment de la communication dans une zone sélectionnée.

Cette disposition est utile afin de pouvoir disposer des données se rapportant aux communications d'auteurs d'infractions commises dans l'une des zones visées ainsi que celles se rapportant à d'éventuels coauteurs ou complices qui n'ont pas accompagné le ou les auteur(s) sur les lieux de l'infraction, ou qui n'y demeuraient pas jusqu'à la consommation de l'infraction, mais avec lesquels il(s) étai(en)t en contact avant, pendant ou après les faits.

Ces données sont en effet primordiales pour permettre l'identification des personnes impliquées dans la commission des infractions poursuivies, la détermination de leurs rôles respectifs ainsi que leur éventuelle localisation après la commission des faits.

L'article prévoit aussi la possibilité d'une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation en cas de menace terroriste atteignant au moins le niveau 3 prévu au plan gouvernemental de vigilance nationale. Eu égard à la gravité d'une telle menace, une telle conservation des données semble proportionnée et justifiée.

L'article proposé prévoit des sanctions pénales en cas de non-respect des obligations résultant dudit article.

La nécessité de cette disposition découle notamment du fait que le comportement d'un tiers qui refuserait de se conformer aux dispositions de l'article risquerait de nuire gravement à une enquête pénale en cours et le cas échéant de favoriser la commission d'un nouveau crime ou d'un nouveau délit. Un tel comportement serait en outre de nature à constituer une menace pour la sécurité publique.

Il se posera encore la question de savoir si les sanctions prévues ne devraient pas être majorées dans l'hypothèse où un refus de se conformer aux dispositions de l'article a favorisé la commission d'un nouveau crime ou d'un nouveau délit, compte tenu de la gravité des conséquences d'une telle inobservation.

Un traitement de données contraire aux dispositions de cet article serait aussi sanctionné par une peine d'emprisonnement et/ou d'amende. En plus, la cessation d'un tel traitement contraire aux dispositions de l'article examiné sera soumis au contrôle de la juridiction saisie. L'article ne précise pas quelles juridictions seront compétentes pour se prononcer sur la cessation d'un tel traitement de données. S'agirait-il d'une juridiction pouvant être saisie par voie directe, par exemple en cas d'infraction constatée à l'article 5bis, ou la question de la cessation d'un tel traitement pourrait-elle également être soulevée de manière incidente par exemple devant une juridiction d'instruction appelée à examiner la régularité d'un acte d'instruction dans le cadre d'un recours juridictionnel dirigé contre cet acte ?

Article 2 5°

Cet article adapte les références textuelles en fonction des modifications législatives réalisées ou à réaliser et ne suscite pas d'observation particulière.

Article 2 6°

Cet article modifie l'article 5-2 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, devenant l'article 5quater, ne suscite pas d'observations.

Article 2 7°

Cet article modifie l'article 7, paragraphe 5bis de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, afin d'étendre le champ d'application de cet article aux communications d'urgence, en englobant au-delà des appels téléphoniques visées jusqu'à présent, les SMS d'urgence. Cette disposition n'appelle pas d'observation particulière.

Article 2 8°

L'article proposé modifie l'article 9 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, afin de transposer en droit interne les principes posés par la jurisprudence de la CJUE, en matière de traitement des données à caractère personnel dans le secteur des communications électroniques.

Cet article transpose l'interdiction d'une conservation généralisée et indifférenciée des données de localisation autres que les données relatives au trafic. Il introduit la possibilité d'une conservation ciblée des données de localisation dans le domaine de la recherche, de la constatation et de la poursuite d'infractions pénales.

Il est renvoyé aux développements faits sous l'article 2 3° qui valent tant en matière de conservation des données relatives au trafic qu'en matière de conservation des données de localisation.

Article 2 9°

L'article proposé modifie l'article 10ter de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, et fait application du principe posé par le juge de l'Union aux termes duquel une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de communications électroniques est admise.

L'article en question détaille les données d'identification qui doivent être conservées par tout fournisseur de communications électroniques ou opérateur, à savoir :

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

- 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 ;
- L'identité internationale d'abonné mobile (IMSI) :
- L'identité internationale d'équipement mobile (IMEI).

Toutes ces données constituent des données d'identification qui ne fournissent pas d'informations sur la communication en soi, ni sur son contenu, ni sur la localisation de l'usager concerné et sont donc moins intrusives dans la vie privée que les données relatives au trafic et à la localisation.

En même temps, ces données n'auront pas la même utilité dans le cadre d'une enquête pénale que les données relatives au trafic et à la localisation, dans la mesure où elles ne contiennent par exemple pas d'informations au sujet des questions primordiales dans des enquêtes pénales, telles que des informations sur d'éventuels déplacements d'une personne suspectée ou de contacts téléphoniques de cette dernière.

L'article proposé prévoit en outre une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une communication, pour une période temporellement limitée à 6 mois pour les besoins de sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave.

L'adresse IP à la source de la connexion est essentielle dans le cadre de certaines enquêtes judiciaires, notamment en cas d'exercice de poursuites du chef d'infractions aux articles 383, 383bis, 383ter et 384 du Code pénal. L'adresse IP à la source d'une connexion permettra l'identification de l'équipement informatique à partir duquel une communication au moyen de l'Internet est effectuée et permettra ainsi de déterminer la personne qui a diffusé ou téléchargé des images ou messages prohibés en vertu des articles 383 et suivants du Code pénal.

L'identification d'un usager en vertu de l'adresse IP attribuée à la source aura également toute son importance dans le cadre des enquêtes pénales concernant des faits de cybercriminalité tels qu'escroqueries commises via Internet ou infractions aux articles 509-1 et suivants du Code pénal, qui ne cessent de se multiplier avec l'essor des technologies et des moyens de communications modernes. Cette donnée peut également être utile pour l'identification d'auteurs de messages publiés ou proférés par l'Internet qui sont susceptibles de constituer des propos incitant à la haine, des propos constitutifs d'harcèlement obsessionnel ou des propos calomnieux ou diffamatoires.

L'article proposé prévoit des sanctions pénales en cas de non-respect des obligations résultant dudit article.

Il est à ce sujet renvoyé aux observations faites sous l'article 2 4°.

*

Article 3

Les modifications qu'apportera l'article 3 du projet à la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat n'appellent pas d'observations particulières de la part du Parquet Général.

*

Article 4

Cet article prévoit que la commission consultative dont la création est prévue aux termes de paragraphe 4 de l'article 5bis de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, 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

Cet article de technique législative n'appelle pas d'observations.

Article 6

L'article proposé fixe le délai d'entrée en vigueur de la future loi et ne requiert aucune observation particulière, sauf à relever que le délai prolongé, accordé par les auteurs du projet de loi aux opérateurs et fournisseurs concernés, semble nécessaire pour permettre à ces derniers de s'adapter aux nouvelles dispositions à venir, lesquelles traduisent un véritable changement de paradigme en la matière.

Le respect des délais prévus à l'article 4 du projet de loi ainsi qu'une date d'entrée en vigueur éloignée devront permettre la mise en place par les acteurs concernés d'un système qui est fonctionnel dès le premier jour de l'entrée en vigueur de la nouvelle loi alors qu'une perte des données à conserver de manière ciblée en raison de déficiences au niveau de la transposition des nouvelles mesures législatives risquerait tout simplement d'avoir des conséquences extrêmement dommageables pour la sécurité nationale et l'ordre public.

Luxembourg, le 13 mars 2023

Pour le Procureur général d'Etat,
L'avocat général
Bob PIRON

Impression: CTIE – Division Imprimés et Fournitures de bureau

8148/01

N° 8148[1]

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 électroniques ; et

3° de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat

* * *

AVIS DE LA COUR D'APPEL

(30.4.2023)

Vu le courrier de Madame le Procureur Général d'Etat du 6 février 2023, requérant l'avis de Monsieur le Président de la Cour supérieure de justice sur 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'État.

Vu le transmis de Monsieur le Président de la Cour supérieure de justice du 8 février 2023.

Le présent projet de loi a pour objet de réglementer la rétention de données à caractère personnel générées ou traitées par l'utilisation de services de communications électroniques d'une manière à ce que soient conciliés, d'une part, la protection des droits fondamentaux des personnes privées, notamment leur vie privée, et, d'autre part, la sauvegarde de la sécurité nationale, de la défense et de la sécurité publique qui implique une ingérence dans l'exercice de ces droits fondamentaux, ce à la lumière des exigences des derniers arrêts de la Cour de Justice de l'Union Européenne en la matière (arrêts « Digital Rights Ireland et Seitlinger » du 8 avril 2014, « Tele2 et Watson » du 21 décembre 2016, « Quadrature du Net et FON », « Privacy International » du 6 octobre 2020 et « Commissioner of the Garda Siochàna e.a. » du 5 avril 2022 et « SpaceNet » et « VD » du 20 septembre 2022). Il s'agit de garantir un équilibre entre la conservation et l'accès aux données traitées par les fournisseurs de communications électroniques dans le cadre de la lutte contre le terrorisme et la criminalité grave et la protection de la vie privée des personnes physiques.

Seules, les modifications apportées au Code de procédure pénale seront examinées.

Le projet de loi introduit dans ce code un nouvel article 24-3, qui permet au Procureur d'Etat d'ordonner dans le cadre de la recherche et de la poursuite d'un certain type d'infractions pénales (ciblées comme étant celles emportant une peine criminelle ou une peine correctionnelle d'un maximum égal ou supérieur à un an d'emprisonnement) aux opérateurs de télécommunications ou fournisseurs de services de communications électroniques de procéder à la conservation de données de trafic et de localisation, suivant des critères déterminés conformément à la jurisprudence de la Cour de Justice de l'Union Européenne. Il s'agit de préserver ces données afin que les autorités judiciaires puissent y avoir accès ultérieurement, par le biais de l'article 67-1 du Code de procédure pénale. La durée de la mesure de conservation est limitée à six mois, durée qui peut être renouvelée. En cas d'urgence, cette conservation peut être ordonnée verbalement mais doit être confirmée par écrit dans les plus brefs délais. Les données conservées sont détruites lorsque la mesure de conservation prend fin.

Ce nouvel article n'appelle pas d'observations particulières.

En ce qui concerne l'article 48-27 du Code de procédure pénale, un nouveau paragraphe (2) est introduit. Il porte sur l'accès du procureur d'Etat ou du juge d'instruction aux données conservées sur base de l'article 10 ter de la loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques en vue de l'identification de l'utilisateur d'une adresse IP. Il complète la notion de « télécommunications » par la notion de « communications électroniques ».

Il est à noter que le point (1) de cet article vise de manière générale l'enquête pour crime ou délit ou l'instruction préparatoire, tandis que le nouveau point (2) est plus restrictif puisqu'il vise l'enquête pour crime ou délit ou l'instruction préparatoire, mais pour des faits emportant « une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement ».

La modification de l'article 67-1 du Code de procédure pénale vise l'accès du juge d'instruction aux données de trafic et de localisation conservées par les opérateurs de télécommunications ou fournisseurs de services de communications électroniques conformément à la loi du 30 mai 2005 précitée et également au titre du nouvel article 24-3 du Code de procédure pénale. Cet accès auxdites données est limité aux faits sanctionnés par une peine criminelle ou une peine d'emprisonnement dont le maximum est égal ou supérieur à une année.

Cette disposition ne suscite pas d'observation particulière, sauf à préciser que la possibilité d'un recours contre une ordonnance rendue par le juge d'instruction, déjà prévu par l'article 67-1 du Code de procédure pénale dans sa version antérieure au présent projet de loi, reste maintenue.

Pour les présidentes des 5ème, 6ème
et 10ème chambres de la Cour d'appel
(signature)

Impression: CTIE – Division Imprimés et Fournitures de bureau

8148/03

N° 8148[3]

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 électroniques ; et

3° de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat

* * *

AVIS COMMUN DES PARQUETS DU TRIBUNAL D'ARRONDISSEMENT DE LUXEMBOURG ET DE DIEKIRCH

(13.4.2023)

Le projet de loi sous examen entend conformer la législation nationale a la jurisprudence récente de la Cour de justice de l'Union européenne (ci-après CJUE) en matière de rétention des données dans le secteur des communications électroniques. Il répond ainsi a la nécessite, maintes fois rappelée par la jurisprudence européenne, d'une réglementation légalement contraignante en droit interne, devant préciser dans quelles circonstances et sous quelles conditions la rétention des données à caractère personnel et l'accès des autorités nationales à celles-ci est autorisée.

L'élaboration d'un tel cadre légal s'avère particulièrement épineuse, tant la jurisprudence de la CJUE en la matière est complexe et a bouleverse l'approche communément suivie par les Etats membres en matière de conservation des données électroniques aux fins de lutte contre la criminalité. Elle l'est d'autant plus que de nombreuses questions restent ouvertes, alors même qu'elles se trouvent au cœur du nouveau cadre légal que le présent pro jet de loi s'efforce de bâtir. Que faut-il entendre par « criminalité grave » ? L'accès par les autorités nationales aux données d'identité civile couplées aux adresses IP des utilisateurs doit-il être soumis au contrôle préalable d'une juridiction ou d'une autorité administrative indépendante ? Dans quelle mesure les principes dégagés en matière de conservation et accès aux données détenues par les fournisseurs de services de communication électronique s'appliquent-elles à l'exploitation de données numériques stockées dans un téléphone portable ? C'est là un échantillon des questions préjudicielles pendantes devant la CJUE[1], dont les réponses vont inévitablement déterminer la légalité des dispositions sous examen.

Dans ce contexte, il nous paraît essentiel d'adopter une approche pragmatique. Tout d'abord parce qu'il ne suffit pas d'opérer une « transposition » fidèle de la jurisprudence européenne en droit national, si le résultat d'une telle législation complexifie les procédures à outrance sans permettre la collecte de données essentielles à l'aboutissement des enquêtes et des poursuites pénales. Mais aussi parce que des solutions sans doute commodes d'un point de vue opérationnel, mais non conformes à la jurisprudence de la CJUE, risquent d'engendrer des contestations systématiques des mesures d'enquête et aboutir ainsi à des situations de blocage. C'est dans cet esprit que le présent avis se focalisera sur les aspects du projet de loi qui touchent aux procédures pénales.

---

1 Il est fait notamment référence aux affaires pendantes C-470/21, *La Quadrature du Net e.a.,* aff. C-548/21, *C.G./Bezirkshauptmannschaft Landeck*, aff. C-178/22, *Procédure pénale contre inconnus,* aff. C-241/22, *Procédure pénale contre DX.*

Ad article 1er du projet de loi

• *Ad nouvel article 24-3 CPP*

Le nouvel article 24-3 du code de procédure pénale (ci-après CPP) introduit la possibilité pour le Procureur d'Etat d'enjoindre aux opérateurs de télécommunications et aux fournisseurs d'un service de communications électroniques de conserver des données relatives au trafic et à la localisation, afin qu'elles puissent, en cas de besoin, être communiquées aux autorités judiciaires et utilisées par celles-ci dans le cadre d'une enquête, d'une instruction et des poursuites pénales. La disposition permettra ainsi de « geler » de manière ciblée des données avant que celles-ci ne soient effacées ou rendues anonymes par les opérateurs et fournisseurs auxquels s'adresse l'injonction. Il va de soi que la durée de conservation des données relatives au trafic et à la localisation par ces mêmes acteurs, telle qu'établie par la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques (ci-après loi Telecom), aura une incidence directe sur l'efficacité de l'injonction. Il est renvoyé sur ce point aux observations à l'article 2 du projet de loi formulées ci-après.

Soulignons que l'injonction dite « *quick freeze* » porte uniquement sur la conservation des données et non pas sur leur communication aux autorités judiciaires. Tel que le soulignent les auteurs du projet de loi, l'accès se fait dans les conditions prévues par l'article 67-1 CPP. Pourtant, le second alinéa de l'article 24-3 CPP renvoie à un règlement grand-ducal qui détermine les catégories de données pouvant faire l'objet de la mesure de conservation et qui « *peut également déterminer les formes et les modalités suivant lesquelles les données visées sont à mettre à disposition des autorités judiciaires* ». Afin d'assurer la cohérence et lisibilité du texte, il serait opportun, d'une part, de renvoyer explicitement 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, que les auteurs du projet de loi visent dans leurs commentaires. D'autre part, la dernière phrase du second alinéa de l'article 24-3 CPP concernant l'accès aux données devrait être remplacée par un renvoi à l'article 67-1CPP. C'est d'ailleurs une disposition similaire qui figure au dernier paragraphe de l'article 39*quinquies* du Code d'instruction criminelle (ci-après CIC) belge, dont la disposition sous examen est inspirée[2].

---

2 L'article 39*quinquies* du CIC belge se lit comme suit:

« § 1er. Lors de la recherche de crimes et délits, le procureur du Roi peut, s'il existe des indices sérieux que les infractions peuvent donner lieu à un emprisonnement correctionnel principal d'un an ou à une peine plus lourde, ordonner, par une décision écrite et motivée, à un ou plusieurs acteurs visés à l'alinéa 2, de conserver les données vis es à l'article 88bis, § 1, alinéa 1er, générées ou traitées par eux dans le cadre de la fourniture des services de communications concernés, qu'il juge nécessaires.

L'ordre visé à l'alinéa 1er peut être donné, directement ou par l'intermédiaire du service de police désigné par le Roi, à:

- *l'opérateur d'un réseau de communications électroniques; et*
- *toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.*

La décision écrite et motivée mentionne:

- *le nom du procureur du Roi qui ordonne la conservation;*
- *l'infraction qui fait l'objet de l'ordre;*
- *les circonstances de fait de la cause qui justifient la conservation;*
- *l'indication précise d'un ou de plusieurs des éléments suivants: la personne ou les personnes, les moyens de communication ou les lieux qui font l'objet de la conservation;*
- *le cas échéant, les catégories de données de trafic et de localisation qui doivent être conservées;*
- *la durée de la mesure, qui ne peut excéder deux mois à compter de la date de l'ordre, sans préjudice de renouvellement;*
- *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 acteurs visés au paragraphe 1er, alinéa 2, veillent à ce que l'intégrité, la qualité et la disponibilité des données soit garantie et à ce que les données soient conservées de manière sécurisée.

§ 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 coopérer, ou qui fait disparaître, détruit ou modifie les données conservées, est punie d'une amende de cent euros à trente mille euros.

§ 4. L'accès aux données conservées conformément à cet article n'est possible qu'en application de l'article 88bis. »

Afin d'assurer la proportionnalité de la mesure, l'injonction de conservation doit être motivée, suivant le troisième alinéa de l'article 24-3 CPP, et contenir des indications précises permettant d'en délimiter la portée, qu'il s'agisse des personnes, moyens de communication ou lieux visés pour les besoins de l'enquête. La disposition n'opère en revanche aucune distinction entre les données qui sont déjà à disposition des opérateurs et fournisseurs au moment de l'injonction et celles qu'ils génèrent et traitent une fois l'injonction notifiée. A première vue, seule la première catégorie semblerait être visée, le nouvel article 24-3, alinéa 3, lettre c) se limitant à fixer la durée de conservation des données objet de l'injonction. Pourtant, les commentaires à l'article sous examen précisent « *qu'il s'agit donc d'une sorte de « quick freeze » pour le futur* ».

Il est donc essentiel de clarifier ce point en incluant non seulement le « *quick freeze* » des données existantes, mais également le « *future freeze* » pour les données qui seront générées après l'injonction, à l'instar des modifications que l'article 3 du projet de loi envisage d'apporter à l'article 7-1 (1) de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat. Le nouvel article 24-3 du CPP permettrait ainsi au Procureur d'Etat de :

(i) enjoindre immédiatement la conservation des données d'ores et déjà générées et traitées par les opérateurs et fournisseurs dans l'attente qu'un juge d'instruction prenne une ordonnance sur base de l'article 67-1 CPP, soit dans le cadre d'une instruction, soit dans le cadre d'une mini-instruction sur fondement de l'article 24-1 (1), alinéa 3 CPP. Cette option présente dès lors un intérêt pratique lorsque le repérage de télécommunications ou des communications électroniques par le juge d'instruction risque d'être ordonné tardivement, l'injonction de conservation des données permettant alors d'en assurer la disponibilité ;

(ii) enjoindre la conservation des données générées à partir de la date de l'injonction, tel que prévu par l'article 39*quinquies* du CIC belge. Cela permettrait notamment d'assurer la disponibilité des données relatives aux trafic et à la localisation visant une personne, lorsque ces mêmes données ne sont pas conservées par les opérateurs et fournisseurs à des fins commerciales ou en raison des zones géographiques, tel que prévu aux articles 5 et 5*bis* de la loi Telecom. C'est aussi la raison pour laquelle, d'après la disposition belge susvisée, l'injonction doit préciser non seulement la durée de conservation des données, à l'instar du texte luxembourgeois. Elle doit également indiquer « *la durée de la mesure, qui ne peut excéder deux moins à compter de la date de l'ordre, sans préjudice de renouvellement* »[3]. Ainsi par exemple, le ministère public peut enjoindre la conservation des données générées ou traitées au cours des deux mois à compter de la date de l'injonction, lesdites données pouvant être conservées pour une durée maximale de six moins renouvelables.

Il ressort enfin de la jurisprudence de la CJUE que les injonctions de type « *quick freeze* » peuvent être prises « *au moyen d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif* »[4]. S'il ne fait aucun doute que le Procureur d'Etat est le mieux à-même d'ordonner la conservation des données dès les premières phases et selon les besoins de l'enquête, le contrôle par une juridiction de la légalité de l'injonction dépendra vraisemblablement de l'éventuelle utilisation des données ainsi conservées à un stade ultérieur de la procédure pénale. Est-ce qu'un contrôle exercé par la juridiction saisie au fond est suffisant au regard du droit de l'Union ? Dans l'hypothèse où les données dont la conservation est ordonnée ne sont pas communiquées ou utilisées par la suite comme preuve, l'absence de recours juridictionnel direct contre l'injonction prise sur fondement de l'article 24-3 CPP constitue+ elle une violation du droit de l'Union ? Notons que dans les commentaires à l'article, les auteurs du projet de loi ne prennent pas position sur la question, la CJUE n'ayant pas à notre connaissance apporté des éclaircissements sur la question.

• *Ad nouvel article 48-27 CPP*

Le nouvel article 48-27 CPP réglemente, dans son paragraphe 1er, l'accès des autorités judiciaires aux données relatives à l'identité civile des utilisateurs des services de télécommunications et de communications électroniques. Le second paragraphe de la disposition prévoit quant à lui la possibilité pour le procureur d'Etat et le juge d'instruction de requérir le concours d'un opérateur de télécommunications ou d'un fournisseur d'un service de communications électroniques aux fins d'identifier l'utilisateur d'une adresse IP. Tel que le confirment les commentaires à l'article sous examen, cela implique l'accès par le procureur d'Etat aux données conservées sur base de l'article 10*ter* (2) de la

3 Art. 39*quinquies*, §1, alinéa 3 CIC belge.

4 CJUE, arrêt du 5 avril 2022, *Commissioner of An Garda Síochána*, aff. C-140/20, §83.

loi Telecom. Cette disposition vise plus précisément les adresses IP à la source de la connexion qui, selon la jurisprudence européenne, peuvent faire l'objet d'une conservation généralisée « *quoique faisant partie des données relatives au trafic* »[5].

Or, l'accès direct par le Procureur d'Etat à des données d'identité civile couplées à des adresses IP figure parmi les questions ouvertes que la CJUE devra dans un futur proche trancher. Dans les arrêts *Prokurattur et Commissioner of An Garda Síochána*, la Cour a jugé que l'accès des autorités nationales compétentes aux données conservées doit être « *subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante et que la décision de cette juridiction ou de cette entité intervienne à la suite d'une demande motivée de ces autorités présentées, notamment dans Je cadre de procédure de prévention, de détection ou de poursuites pénales* »[6]. Ce contrôle juridictionnel ex-ante ne saurait toutefois pas, aux yeux de la Cour, être exercé par le ministère public qui ne présente pas les garanties d'indépendance requises en raison du rôle qu'il remplit dans le cadre d'une procédure pénale[7]. Dans ces affaires, la question visait cependant l'accès aux données relatives au trafic et à la localisation. Il n'est dès lors pas certain que l'exigence de contrôle juridictionnel préalable s'impose lorsque l'accès porte sur les adresses IP.

Telle est précisément l'une des questions préjudicielles que le Conseil d'Etat français a posé dans une nouvelle affaire *La Quadrature du Net e.a.* qui demeure à ce jour pendante. Il nous semble à cet égard important de souligner que dans ses conclusions du 27 octobre 2022, l'avocat général Szpunar suggère à la CJUE un assouplissement de son approche au « *risque d'une impunité systémique pour les infractions constituées exclusivement en ligne* » et compte tenu des « *difficultés pratiques* » qu'elle soulève[8]. Il estime que l'accès aux données d'identité civile couplées aux adresses IP des utilisateurs ne devrait pas être soumis à un contrôle juridictionnel préalable[9]. Il s'ensuit que la conformité du nouvel article 48-27 CPP au droit de l'Union dépendra sur ce point de la position que la CJUE adoptera dans cette affaire.

• *Ad nouvel article 67-1 CPP*

Les modifications que le présent projet de loi envisage d'apporter à l'article 67-1CPP ont notamment pour objectif d'assurer l'accès par le juge d'instruction aux données que détiennent, traitent ou génèrent les opérateurs de télécommunications et les fournisseurs de services de communications électroniques. A l'instar du nouvel article 24-3 CPP, la durée de conservation des données relatives au trafic et à la localisation ainsi que des adresses IP fixée par la loi Telecom aura inévitablement un impact sur l'efficacité d'une telle mesure. Il est renvoyé sur ce point aux observations à l'article 2 du projet de loi formulées ci après.

Il ressort en effet des commentaires à l'article sous examen que l'article 67-1 CPP aura vocation à s'appliquer non seulement aux données générées à partir de la date de l'ordonnance du juge d'instruction. Il régira également l'accès aux données générées avant cette date que les opérateurs et fournisseurs auront conservé soit dans les conditions prévues par la loi Telecom, soit en exécution d'une injonction prise par le Procureur d'Etat sur base de l'article 24-3 CPP.

Curieusement le projet de loi n'apporte aucune modification au dernier alinéa de l'article 67-1 CPP, en vertu duquel la mesure prise par le juge d'instruction doit préciser « *la durée durant laquelle elle pourra s'appliquer, cette durée ne pouvant excéder un mois à dater de l'ordonnance* ». Aucune autre indication temporelle n'est apportée, de sorte qu'il ne ressort pas clairement du texte si et dans quelle mesure le juge d'instruction pourra ordonner la communication des données générées au cours des mois précédant l'ordonnance.

---

5 CJUE, arrêt du 6 octobre 2020, *Quatradure du Net*, aff. Jointes C-511/18, C-512/18 et C-520/18, §152.

6 CJUE, arrêt du 2 mars 2021, Prokuratuur, aff. C-746/18, §51; CJUE, arrêt du 5 avril 2022, *Commissioner of An Garda Síochána*, aff. C-140/20, §106

7 CJUE, arrêt du 2 mars 2021, Prokuratuur, aff. C-746/18, §54- 57; CJUE, arrêt du 5 avril 2022, *Commissioner of An Garda Síochána*, aff. C-140/20, §109.

8 Conclusions de l'Avocat général Szpunar dans l'affaire C-470/21, *La Quadrature du Net e.a*., §78

9 Conclusions de l'Avocat général Szpunar dans l'affaire C-470/21, *La Quadrature du Net e.a.*, §90 et ss.

Notons que l'article 88*bis* du CIC belge est bien plus explicite dans sa formulation[10]. Il distingue,

---

10 L'article 88*bis* du CIC belge dispose :

« § 1er S'il existe des indices sérieux que les infractions sont de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde, et lorsque le juge d'instruction 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, il peut faire procéder:

1° au repérage des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées;

2° à la localisation de l'origine ou de la destination de communications électroniques.

Si nécessaire, il peut pour ce faire requérir, directement ou par l'intermédiaire du service de police désigné par le Roi, la collaboration:

- *de l'opérateur d'un réseau de communications électroniques; et*
- *de toute personne qui met à disposition ou offre, sur le territoire belge, d'une quelconque manière, un service qui consiste à transmettre des signaux via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques. Est également compris le fournisseur d'un service de communications électroniques.*

Dans les cas visés à l'alinéa 1er, pour chaque moyen de communication électronique dont [5 les données de trafic]5 sont repérées ou dont l'origine ou la destination de la [5 communication électronique]5 est localisée, le jour, l'heure, la durée et, si nécessaire, le lieu 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, son caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête, dans une ordonnance motivée.

Il précise également la durée durant laquelle la mesure pourra s'appliquer pour le futur, cette durée ne pouvant excéder deux mois à dater de l'ordonnance, sans préjudice de renouvellement et, le cas échéant, la période pour le passé sur laquelle l'ordonnance s'étend conformément au paragraphe 2.

En cas de flagrant délit, le procureur du Roi peut ordonner la mesure pour les infractions visées à l'article 90ter, §§ 2, 3 et 4. Dans ce cas, la mesure doit être confirmée dans les vingt-quatre heures par le juge d'instruction.

S'il s'agit toutefois de l'infraction visée à l'article 137, 347bis, 434 ou 470 du Code pénal, à l'exception de l'infraction visée à l'article 137, § 3, 6°, du même Code, le procureur du Roi peut ordonner la mesure tant que la situation de flagrant délit perdure, sans qu'une confirmation par le juge d'instruction ne soit nécessaire.

S'il s'agit de l'infraction visée à l'article 137 du Code pénal, à l'exception de l'infraction visée à l'article 137, § 3, 6°, du même Code, le procureur du Roi peut en outre ordonner la mesure dans les septante-deux heures suivant la découverte de cette infraction, sans qu'une confirmation par le juge d'instruction soit nécessaire.

Toutefois, le procureur du Roi peut ordonner la mesure si le plaignant le sollicite, lorsque cette mesure s'avère indispensable à l'établissement d'une infraction visée à l'article 145, § 3 et§ 3bis de la loi du 13 juin 2005 relative aux communications électroniques.

En cas d'urgence, la mesure peut être ordonnée verbalement. Elle doit être confirmée dans les plus brefs délais dans la forme prévue aux alinéas 4 et 5.

§ 2. Pour ce qui concerne l'application de la mesure visée au paragraphe 1er, alinéa 1er, aux données de trafic ou de localisation conservées sur la base des articles 126/1 et 126/3 de la loi du 13 juin 2005 relative aux communications électroniques, les dispositions suivantes s'appliquent:

- *pour une infraction visée au livre II, titre Iter, du Code pénal, le juge d'instruction peut dans son ordonnance requérir les données pour une période de douze mois préalable à l'ordonnance;*
- *pour une autre infraction visée à l'article 90ter, §§ 2 à 4, qui n'est pas visée au premier tiret ou pour une infraction qui est commise dans le cadre d'une organisation criminelle visée à l'article 324bis du Code pénal, ou pour une infraction qui est de nature à entraîner un emprisonnement correctionnel principal de cinq ans ou une peine plus lourde, le juge d'instruction peut dans son ordonnance requérir les données pour une période de neuf mois préalable à l'ordonnance;*
- *pour les autres infractions, le juge d'instruction ne peut requérir les données que pour une période de six mois préalable à l'ordonnance.]6]3*

§ 3. La mesure ne peut porter sur les moyens de communication électronique d'un avocat ou d'un médecin que si celui-ci est lui-même soupçonné d'avoir commis une infraction visée au paragraphe 1er ou d'y avoir participé, ou si des faits précis laissent présumer que des tiers soupçonnés d'avoir commis une infraction visée au paragraphe 1er, utilisent ses moyens de communication électronique.

La mesure ne peut être exécutée sans que le bâtonnier ou le représentant de l'ordre provincial des médecins, selon le cas, en soit averti. Ces mêmes personnes seront informées par le juge d'instruction des éléments qu'il estime relever du secret professionnel. Ces éléments ne sont pas consignés au procès-verbal. Ces personnes sont tenues au secret. Toute violation du secret est punie conformément à l'article 458 du Code pénal.

§ 4. Les acteurs visés au§ 1er, alinéa 2, communiquent les informations demandées en temps réel ou, le cas échéant, au moment précisé dans la réquisition, selon les modalités fixées par le Roi, sur la proposition du ministre de la Justice et du ministre compétent pour les Télécommunications.

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 au présent article, concours dont les modalités sont fixées par le Roi, sur la proposition du ministre de la Justice et du ministre compétent pour les Télécommunications, ou ne le prête pas en temps réel ou, le cas échéant, au moment précisé dans la réquisition, est punie d'une amende de cent euros à trente mille euros ».

dans son paragraphe 1er, la captation de données en temps réel, le juge d'instruction étant tenu d'indiquer « *la durée durant laquelle la mesure pourra s'appliquer pour le futur* ». D'autre part, le paragraphe 2 de l'article 88*bis* du CIC belge, délimite le champ d'application de la mesure pour le passé, le juge d'instruction étant explicitement autorisé à requérir les données pour une période allant de 6 à 12 moins préalables à l'ordonnance selon la gravité de l'infraction.

Ad article 2 du projet de loi

• ***Une durée insuffisante de la conservation « par défaut » des données relatives au trafic, à la localisation et des adresses IP***

L'article 2 du projet de loi sous examen définit notamment les obligations de conservation qui s'imposent aux fournisseurs et aux opérateurs de services de communication électroniques indépendamment de toute injonction ou réquisition transmise par les autorités judiciaires. Les délais de conservation « par défaut » inscrits dans la loi Telecom déterminent dès lors la disponibilité d'informations pouvant s'avérer utiles dans le cadre de poursuites pénales. Il est donc fondamental qu'un tel délai soit suffisamment long pour permettre aux autorités judiciaires de réagir tant que les métadonnées sont disponibles, au risque de compromettre l'efficacité des enquêtes et, avec elles, la possibilité effective de poursuivre les auteurs des faits. Cette nécessité est d'autant plus forte lorsque les données en question constituent le seul moyen d'investigation dont disposent les enquêteurs, tel que l'a reconnu la CJUE s'agissant des adresses IP permettant l'identification de personnes impliquées dans les infractions commises en ligne[11]. Rappelons par ailleurs que les données conservées ne sont pas nécessairement incriminantes, mais peuvent aussi disculper un suspect.

Force est toutefois de constater que, hormis les données relatives à l'identité civile des utilisateurs pour lesquelles il est renvoyé au délai de 3 ans prévu à l'article 10*bis*, paragraphe 7 de la loi Telecom[12], son nouvel article 5*bis* (1), alinéa 1er limite la durée de conservation des données relatives au trafic et à la localisation à 6 mois à compter de la communication. Il en irait de même pour les adresses IP, conformément au nouvel article 10*ter* (2), alinéa 2 de la loi Telecom.

Là où la législation belge prévoit des délais de conservation allant jusqu'à un an[13] et la loi française un délai de un an[14], le délai de six mois proposé risque de s'avérer bien trop court et de mettre en échec les investigations, y compris dans les affaires de criminalité grave perpétrées en ligne. Il suffira d'une plainte tardive, dénonçant des faits de pédopornographie via internet bien au-delà des six mois de leur commission, pour que les autorités ne puissent plus accéder à des éléments essentiels aux poursuites. Sans oublier que les affaires de cybercriminalité, telles que des escroqueries perpétrées en ligne par des réseaux organisés, présentent bien souvent des ramifications internationales, les enquêtes devant alors composer avec le temps nécessairement plus long de l'entraide judiciaire.

• ***Le critère problématique des zones géographiques***

Quant aux conditions dans lesquelles la conservation est autorisée, le projet de loi distingue, d'une part, la conservation généralisée des adresses IP prévue par le nouvel article 10*ter* (2) de la loi Telecom et, d'autre part, la conservation ciblé des données relatives au trafic et à la localisation régie par le nouvel article 5*bis* de la loi Telecom. Cette seconde disposition viserait, d'après le commentaire des articles, les métadonnées définies par le 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. Dans un souci de lisibilité, la référence exacte audit règlement pourrait être insérée au troisième alinéa du nouvel article 5*bis* (1) de la loi Telecom.

Plus problématiques sont cependant les critères délimitant les zones géographiques au sein desquelles les données seront exceptionnellement conservées. L'approche choisie par les auteurs du projet de loi est calquée sur les critères déterminant les zones dans lesquelles la vidéosurveillance peut être autorisée conformément à l'article 43*bis* de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale.

---

11 CJUE, arrêt du 6 octobre 2020, *Quatradure du Net*, aff. Jointes C-511/18, C-512/18 et C-520/18, §154.

12 Nouvel article 10*ter* de la loi Telecom.

13 Voy. notamment les art. 126 et 126/3 de la loi modifiée du 13 juin 2005 relative aux communications électroniques.

14 Art. L.34-1 du Code des postes et des communications électroniques.

Il importe de noter que dans ce contexte la collecte de données fait face à une contrainte technique différente : elle présuppose en amont l'installation de caméras de surveillance dans le périmètre concerné, la captation d'images étant dès lors par définition ciblée. A l'inverse, les réseaux de télécommunications couvrent d'ores et déjà l'ensemble du territoire national. C'est sans doute pourquoi la jurisprudence européenne se montre exigeante quant à l'élaboration d'un critère géographique devant être suffisamment précis pour que sa mise en œuvre n'aboutisse dans les faits à une conservation généralisée et indifférenciée des métadonnées[15]. Les Etats membres doivent plus précisément se fonder sur des « *éléments objectifs et non discriminatoires* » indiquant « *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* »[16]. Ainsi par exemple, le taux moyen de criminalité grave peut légalement circonscrire la conservation des données dans une zone géographique, à condition que la mesures soit sujette à modification en fonction de l'évolution dudit taux[17].

Il résulte toutefois du nouvel article 5*bis* (2), point 1°, lettre a) de la loi Telecom que la conservation ciblée de données relatives au trafic et à la localisation sera notamment possible dans « *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* ». Il n'est fait référence à aucun seuil prédéfini, aucune différenciation plus détaillée selon la gravité des infractions, alors même que le législateur belge a estimé devoir préciser cela dans la loi[18].

Particulièrement flou est aussi le critère inscrit à la lettre d) de l'article 5*bis* de la loi Telecom, qui vise « *les lieux qui par leur nature rassemblent un grand nombre de personnes* ». Que faut-il entendre par « *un grand nombre* » ? Quels lieux sont « *par leur nature* » visés ? Est-ce que les espaces dédiés aux festivals en plein air organisés chaque année à travers le pays tombent dans cette catégorie ?

Curieusement les infrastructures sensibles d'intérêt national, tels que les barrages de la Haute-Sûr et de l'Our ou le Centre militaire à Diekirch, ne sembleraient pas en tant que telles visées par le nouvel article 5*bis* 1° de la loi Telecom. Ces sites tomberaient dans le champ géographique de rétention des données uniquement en cas de menace terroriste de niveau 3 sur le plan « VIGILNAT » et à condition que ladite menace couvre l'ensemble du territoire, tel que prévu au point 2° de la disposition.

S'agissant de la procédure à suivre, le second alinéa de la disposition précitée fait vaguement référence à une proposition déterminant l'étendue du périmètre de chaque zone géographique qu'une commission consultative, dont la composition n'est pas précisée, devra soumettre tous les trois ans au Haut Commissariat à la protection nationale. S'agit-il de procéder à une analyse d'impact, à l'instar de ce que prévoit l'article 43*bis* de la loi modifiée du 18 juillet 2018 sur la Police grand-ducale, qui devra s'appuyer sur les statistiques disponibles ? Si la conservation ciblée des données relatives au trafic et la conservation est un élément clé de la présente réforme qui a pour but d'assurer la conformité de la législation nationale au droit de l'Union, ces questions méritent à notre sens d'être précisées, au risque d'engendrer une législation dès le départ susceptible d'être invalidée. L'enjeu est ici de taille, car à défaut de données conservées les autorités judiciaires pourraient se trouver dans l'impossibilité d'accéder aux éléments de preuves sur lesquelles reposent les poursuites contre toute sorte d'infraction commise en ligne.

Il est également essentiel que les autorités qui de par leur mission disposent de l'expertise et des informations nécessaires à la délimitation des zones exposées à un risque élevé de criminalité grave, puissent contribuer au processus. Cela est d'autant plus crucial que la conservation ciblée par zones géographiques va inévitablement déboucher dans un niveau de protection des données personnelles, mais aussi des capacités d'actions de la police et du Parquet à géométrie variable. Alors qu'au sein des zones géographiques définies selon les critères du nouvel article 5*bis*(2) de la loi Telecom la détection, la recherche et la poursuite des infractions pourra s'appuyer sur tous les moyens d'investigation techniques à disposition, tel ne serait pas le cas d'un grand nombre de dossiers rattachés à des zones « non couvertes » et pour grande partie rurales. En pratique, selon que le domicile de l'auteur ou de la victime se trouvent dans le périmètre en question, il sera matériellement possible de localiser une connexion, vérifier la fréquence des communications ou encore leur destinataire. Les moyens dont les autorités disposeront pour enquêter sur des infractions, telles que des cambriolages, des crimes violents ou encore

15 CJUE, arrêt du 5 avril 2022, *Commissioner of An Garda Síochána*, aff. C-140/20, §83.

16 *Ibidem*, §79-80.

17 *Ibidem*, §82 AG

18 Art. 126/3 de la loi modifiée du 13 juin 2005 relative aux communications électroniques.

du harcèlement, seront d'office plus étendus dès lors qu'ils seront commis, par exemple, aux alentours d'infrastructures d'envergure nationale. Ils dépendront à l'inverse de la conservation opérée par les fournisseurs et opérateurs de services de communications électroniques à des fins commerciales ou de facturation, si les faits ne sont pas rattachés à de telles zones.

Luxembourg, le 13 avril 2023

Georges OSWALD
Procureur d'Etat à Luxembourg

Ernest NILLES
Procureur d'Etat à Diekirch

Impression: CTIE – Division Imprimés et Fournitures de bureau

8148/05

N° 8148[5]

CHAMBRE DES DEPUTES

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

* * *

AVIS DU CONSEIL D'ETAT

(23.1.2024)

Par dépêche du 8 février 2023, le Premier ministre, ministre d'État, a soumis à l'avis du Conseil d'État le projet de loi sous rubrique, élaboré par la ministre de la Justice.

Au texte du projet de loi étaient joints un exposé des motifs, un commentaire des articles, une fiche d'évaluation d'impact, une fiche financière indiquant que le projet en question ne comportait pas de disposition dont l'application serait susceptible de grever le budget de l'État, ainsi qu'une version coordonnée, par extraits, des textes législatifs que le projet émargé tend à modifier.

L'avis commun des procureurs d'État près du Tribunal d'arrondissement de Luxembourg et du Tribunal d'arrondissement de Diekirch, ainsi que les avis du procureur général d'État, de la Cour d'appel et du Tribunal d'arrondissement de Luxembourg sont parvenus au Conseil d'État en date du 2 mai 2023.

L'avis de la Commission nationale pour la protection des données n'est pas encore parvenu au Conseil d'État au moment de l'adoption du présent avis.

*

CONSIDERATIONS GENERALES

La loi en projet vise à adapter les actes de transposition nationaux de 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), ci-après la « directive 2002/58/CE », en les rendant conformes à l'interprétation de cette directive par la Cour de justice de l'Union européenne.

Tant les auteurs du projet de loi sous avis que la cellule scientifique de la Chambre des députés, dans son « Aperçu scientifique » n° CS-2022-DR-030[1], ont fait un résumé des principales conséquences de l'arrêt rendu par la Cour de Justice de l'Union européenne, siégeant en grande chambre, le 8 avril 2014, *Digital Rights Ireland et Seitlinger e.a.*, qui a déclaré invalide la directive 2006/24/CE 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, ainsi que des autres arrêts de principe qui y ont fait suite, de telle sorte qu'une nouvelle analyse par le Conseil d'État ne s'impose pas sur ces points.

1 https://www.chd.lu/sites/default/files/2023-02/Conservation%20donn%C3%A9es%20de%20connexion.pdf.

Ces décisions rendent nécessaire une réforme du droit interne luxembourgeois afin d'assurer la conformité de celui-ci avec le prescrit du droit européen, tel qu'interprété par le juge européen. Il s'agit des dispositions issues 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[2], ayant transposé la prédite directive. Il s'agit essentiellement de mettre en place une meilleure mise en balance des différents intérêts publics et privés en jeu.

Les juges européens ont ainsi retenu, pour l'essentiel, qu'une conservation généralisée et indifférenciée ainsi qu'une exploitation des métadonnées issues de communications électroniques, même à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales, sans autres limitations ni contrôles, ne sont pas conformes aux principes de droit européen, et, plus particulièrement, ne sont pas permises par l'article 15, paragraphe 1er, de la directive 2002/58/CE. Une telle conservation, pour être admise, devrait, au contraire, respecter les conditions strictes dégagées par les arrêts de la Cour de justice de l'Union européenne (notamment les arrêts C-623/17, C-511/18, C-512/18, C-520-18 et C-140/20) et en tenant compte des types de données visées ainsi que du but de la conservation.

Toutefois, ainsi que le souligne le procureur général d'État dans son avis du 13 mars 2023, « le recours aux données relatives au trafic et à la localisation des communications[3] constituent des moyens efficaces, souvent primordiaux dans la lutte contre la criminalité grave et/ou organisée, qui constitue une menace grave, actuelle et réelle pour les citoyens. Il s'agit dans un nombre important de cas d'une condition déterminante du succès des enquêtes menées et il n'existe pas de méthodes d'enquête alternatives qui pourraient s'y substituer de manière efficace. » Un certain nombre d'exemples de dossiers sont cités à l'appui de ce constat dont on peut par ailleurs admettre qu'il vaut également pour le Service de renseignement de l'État, confronté, dans les limites de ses compétences, à des problèmes similaires.

*

EXAMEN DES ARTICLES

Article 1er

Point 1°

La disposition sous revue vise à insérer un nouvel article 24-3 au Code de procédure pénale, traitant notamment de la conservation de données relatives au trafic et à la localisation des utilisateurs de services de télécommunications.

Le nouvel article 24-3 du Code de procédure pénale donne pouvoir au procureur d'État, dans le cadre de la recherche et de la poursuite de certaines infractions, d'enjoindre aux opérateurs de conserver, de façon ciblée, certaines données de trafic et de localisation. Cette conservation ne fait qu'éviter que les opérateurs ne procèdent à un effacement desdites données à l'expiration du délai de conservation légalement prévu. Les données conservées restent toutefois stockées dans les systèmes propres des opérateurs concernés jusqu'à un accès par les autorités judiciaires sous les conditions inscrites, selon la nature des données, aux nouveaux articles 48-27 et 67-1 du Code de procédure pénale, modifiés à cette fin par le projet sous avis.

À titre de remarque générale, le Conseil d'État propose de recourir, de préférence, aux termes « enjoindre » et « injonction » en lieu et place des termes « ordonner » et « ordre », étant donné que ces derniers sont réservés à des décisions d'autorités judiciaires de jugement ou d'instruction.

Sur le fond de la disposition sous examen, le Conseil d'État attire, dans un premier temps, l'attention des auteurs sur le fait que la Cour de justice de l'Union européenne a, dans sa jurisprudence relative

2 Mémorial A, n° 122 du 29 juillet 2010.

3 Donc à l'exclusion du contenu même des communications, dont la surveillance reste réglée par des dispositions législatives spécifiques.

à la directive 2002/58/CE[4], précisé qu'une conservation préventive et généralisée de données relatives au trafic et de données de localisation n'est possible qu'en cas de menace grave pour la sécurité nationale, tandis que la conservation des données de façon ciblée est, quant à elle, possible, mais uniquement en cas de menace grave pour la sécurité publique ou pour lutter contre la criminalité grave.

Les auteurs du projet de loi sous avis précisent, dans le commentaire de la disposition, que celle-ci concerne une conservation ciblée. Selon ce projet, une telle conservation ciblée n'est possible que si les conditions inscrites au nouvel article 24-3 sont remplies et notamment les conditions de forme inscrites au paragraphe 1er, alinéa 3, lettre b) qui prévoit que la décision de conservation doit indiquer avec précision un ou plusieurs des éléments suivants : (1) la ou les personnes concernées, (2) les moyens de communication visés ou (3) les lieux qui font l'objet de la conservation.

Le Conseil d'État rappelle toutefois que, selon la Cour de justice de l'Union européenne, il appartient aux États membres de fixer le cadre général dans leur droit national en ce qui concerne ces trois hypothèses, en tenant compte des critères qu'elle a établis dans ses différents arrêts rendus dans la matière concernée, et plus particulièrement pour ce qui est des personnes et des lieux visés.

Par ailleurs, toujours dans l'hypothèse d'une conservation ciblée, la disposition sous examen prévoit que la finalité de cette conservation est « la recherche, […] la constatation et […] 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 ». Elle ne se situe donc pas dans l'une des deux finalités autorisées en cas de conservation ciblée, les infractions sanctionnées par une peine d'emprisonnement égale ou supérieure à un an ne relevant de surcroît pas toutes de la criminalité grave.

Par conséquent, le Conseil d'État s'oppose formellement à la disposition sous examen, dans la mesure où celle-ci est contraire à la directive 2002/58/CE telle qu'interprétée par la Cour de justice de l'Union européenne.

En ce qui concerne la nature des données conservées, le Conseil d'État s'interroge sur les termes « données de l'Internet » utilisés à l'alinéa 2 du paragraphe 1er. S'agit-il notamment de l'adresse IP ? La réponse à cette question est importante, dans la mesure où la Cour de justice de l'Union européenne a précisé que, si les adresses IP relèvent bien de la catégorie de données relatives au trafic et à la localisation, elles obéissent à un régime différent[5], de sorte que la directive 2002/58/CE, telle qu'interprétée par la Cour de justice de l'Union européenne, ne s'opposerait pas à une conservation ciblée dans le cadre de la recherche et de la poursuite d'infractions pénales quelles qu'elles soient. Une conservation généralisée et indifférenciée des adresses IP n'est en revanche admissible qu'en cas de menace grave pour la sécurité publique ou pour la lutte contre la criminalité grave. L'imprécision des termes « données de l'Internet », sans que le contenu de cette notion ne soit suffisamment précisé au niveau de la loi donne dès lors naissance à une insécurité juridique que le Conseil d'État doit rencontrer par une opposition formelle.

Il est vrai que le paragraphe 1er, alinéa 2, renvoie à un règlement grand-ducal pour « détermine[r] 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 » tout en précisant que celui-ci « peut également déterminer les formes et les modalités suivant lesquelles les données visées sont à mettre à la disposition des autorités judiciaires. »

Le Conseil d'État rappelle toutefois que l'article 31 de la Constitution, qui figure dans la section consacrée aux libertés publiques, dispose que « [t]oute personne a droit à l'autodétermination informationnelle et à la protection des données à caractère personnel la concernant. Ces données ne peuvent être traitées qu'à des fins et dans les conditions déterminées par la loi », tandis que l'article 37 de la Constitution précise, dans sa première phrase, que « [t]oute limitation à l'exercice des libertés publiques doit être prévue par la loi et respecter leur contenu essentiel. »

Il s'ajoute à ce rappel des textes fondamentaux que la Cour constitutionnelle, en affinant sa jurisprudence antérieure, a, dans son arrêt n° 177 du 3 mars 2023, retenu que « [d]'après l'article 32,

---

4 Voir, par exemple : CJUE, arrêt du 6 octobre 2020, *La Quadrature du Net e.a. contre Premier ministre e.a.*, C-511/18, C-512/18, C-520/18, ECLI:EU:C:2020:791 ; CJUE, arrêt du 5 avril 2022, *G.D. contre Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources, Attorney General*, C-140/20, ECLI:EU:C:2022:258 ; CJUE, arrêt du 20 septembre 2022, *Bundesrepublik Deutschland contre SpaceNet AG et Telekom Deutschland GmbH*, C-793/19, C-794/19, ECLI :EU :C :2022 :702.

5 *Ibid.*

paragraphe 3[6], de la Constitution, dans les matières réservées par la Constitution à la loi, la fixation des objectifs des mesures d'exécution doit être clairement énoncée, de même que les conditions auxquelles elles sont, le cas échéant, soumises. L'orientation et l'encadrement du pouvoir exécutif doivent, en tout état de cause, être consistants, précis et lisibles, l'essentiel des dispositions afférentes étant appelé à figurer dans la loi. »[7]

Par conséquent, la disposition sous examen, en prévoyant une fixation de la catégorie de données par voie de règlement grand-ducal, sans entourer ce pouvoir du Grand-Duc d'un cadrage normatif suffisant n'est pas conforme aux exigences de la Constitution, de sorte que le Conseil d'État doit s'y opposer formellement.

En ce qui concerne l'article 24-3, paragraphe 1er, alinéa 2, troisième phrase, le Conseil d'État rappelle encore le principe retenu à l'article 31, deuxième phrase, de la Constitution, à savoir que les données à caractère personnel « ne peuvent être traitées qu'à des fins et dans les conditions déterminées par la loi. » Le Conseil d'État comprend que le règlement grand-ducal en question est appelé à régler les éléments moins essentiels de la transmission, de telle sorte que le Conseil d'État peut s'en accommoder.

L'alinéa 3, lettre a), prévoit que le procureur d'État indique dans son injonction « [l]'infraction qui fait l'objet de l'ordre ». Le Conseil d'État s'interroge sur la portée et l'utilité de cette indication, étant donné que, premièrement, il n'appartient pas aux opérateurs d'apprécier la légalité de l'injonction, que, deuxièmement, la qualification pénale des faits objet de la poursuite peut être modifiée au cours de l'enquête ou de l'instruction et qu'enfin et troisièmement, il est contraire notamment à la protection de la vie privée de la personne visée – qui n'est pas nécessairement l'objet de la poursuite pénale – que les opérateurs disposent de cette information. Il insiste par conséquent sur l'omission de cette disposition, dénuée de toute valeur utile.

Toujours à l'alinéa 3, à la lettre c), il est prévu que le délai de conservation est de six mois, mais le texte précise que « [c]e délai peut être prolongé par écrit ». Selon l'interprétation donnée par la Cour de Justice de l'Union européenne dans l'arrêt C 140/20[8], la directive précitée exige que la conservation de données soit effectuée uniquement « pour une période temporellement limitée au strict nécessaire, mais renouvelable ». En prévoyant simplement que le délai peut être prolongé, sans encadrer davantage cette faculté autrement que par la nécessité d'un écrit, la disposition sous examen n'est pas conforme au prescrit européen, tel qu'interprété par la jurisprudence précitée. Elle est en outre source d'insécurité juridique étant donné qu'une prolongation d'un délai, contrairement à sa reconduction, ne donne pas de limite précise à la mesure, entraînant de ce fait une imprécision quant à sa durée. Enfin, si la prolongation vise ici la conservation rapide, il convient de rappeler que celle ci n'est admissible, sous certaines conditions, que pour deux finalités, à savoir la lutte contre la criminalité grave et la sauvegarde de la sécurité nationale. Il s'impose par conséquent, sous peine d'opposition formelle pour contrariété avec la directive 2002/58/CE telle qu'interprétée par la Cour de justice de l'Union européenne, mais encore pour être source d'insécurité juridique, de compléter le texte sous examen dans le sens indiqué.

En ce qui concerne le paragraphe 2, non autrement commenté par les auteurs de la loi en projet, le Conseil d'État s'interroge sur la portée de l'exception portant sur « des données auxquelles on a pu légalement accéder et qui ont été préservées ». Afin d'éviter toute ambiguïté sur cette portée, le Conseil d'État propose la reformulation suivante ;

« […] à l'exception des données qui ont fait l'objet d'une des mesures prévues à l'article 67-1 : ».

Le paragraphe 3 n'appelle pas d'observation.

Point 2°

Sans observation.

---

6 En l'occurrence, il s'agit de l'article 45, paragraphe 3, de la Constitution révisée, à contenu identique sur ce point.

7 Cour constitutionnelle, 3 mars 2023, n° 177, Mém. A n° 127 du 10 mars 2023.

8 Cour de justice de l'Union européenne, arrêt du 5 avril 2022, *G.D. contre Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources, Attorney General,* C-140/20, ECLI:EU:C:2022:258, point 101.

Point 3°

Les modifications proposées n'appellent pas d'observation de fond. Toutefois, le Conseil d'État suggère de faire référence, au paragraphe 2, alinéa 1er, également au « fournisseur d'un service de communications électroniques », au lieu de se borner à viser seulement « chaque fournisseur des services concernés », afin d'augmenter la clarté du texte sous examen.

Article 2

Points 1° et 2°

Sans observation.

Point 3°

Les considérations qui suivent sont communes aux points 3°, 4°, 8° et 9° de l'article 2 sous avis. Ces points ont tous trait à des sanctions pénales en cas de méconnaissance des diverses obligations instaurées par les dispositions en question.

Le Conseil d'État constate que ces dernières dispositions transposent pour l'essentiel les principes prévus par 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), ci-après le « RGPD », en assortissant leur non-respect de sanctions pénales.

Le régime de sanctions prévu par le RGPD repose sur les articles 83 et 84. L'article 83 prévoit une obligation pour les États membres de prévoir des sanctions administratives dans des cas limitativement énoncés aux paragraphes 4 et 5. L'article 84 dispose, en son paragraphe 1er, que ces États « déterminent le régime des autres sanctions applicables en cas de violations du présent règlement, en particulier pour les violations qui ne font pas l'objet des amendes administratives prévues à l'article 83, et prennent toutes les mesures nécessaires pour garantir leur mise en œuvre ». Le considérant 150 du RGPD précise ce qui suit : « L'application d'une amende administrative ou le fait de donner un avertissement ne portent pas atteinte à l'exercice d'autres pouvoirs des autorités de contrôle ou à l'application d'autres sanctions en vertu du présent règlement. »

Il en résulte qu'il est en principe possible de prévoir des sanctions supplémentaires aux amendes administratives, prévues par l'article 83.

Toutefois, en prévoyant des délits pénaux pour la violation d'obligations pouvant déjà entraîner une amende administrative, il ne peut être exclu qu'un même comportement soit sanctionné à la fois de manière administrative par la Commission nationale pour la protection des données[9] et de manière pénale par le juge répressif. Or, il ressort notamment du considérant 149 du RGPD que, pour l'application des obligations découlant de celui-ci, « [l]es États membres devraient pouvoir déterminer le régime des sanctions pénales applicables en cas de violation du présent règlement, y compris de violation des dispositions nationales adoptées en application et dans les limites du présent règlement. Ces sanctions pénales peuvent aussi permettre la saisie des profits réalisés en violation du présent règlement. Toutefois, l'application de sanctions pénales en cas de violation de ces dispositions nationales et l'application de sanctions administratives ne devrait pas entraîner la violation du principe *ne bis in idem* tel qu'il a été interprété par la Cour de justice. »

Le Conseil d'État donne à considérer que le principe du « *ne bis in idem* », garanti notamment par l'article 4 du Protocole n° 7 à la Convention européenne des droits de l'homme[10], s'applique dès lors que sont en cause les mêmes faits, appréciés de façon matérielle, indépendamment des différentes

---

9 La Commission nationale pour la protection des données est compétente pour prononcer des amendes administratives en cas de violation du RGPD en application de l'article 12 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données, qui dispose ce qui suit : « Dans le cadre des missions de l'article 7, la CNPD dispose des pouvoirs tels que prévus à l'article 58 du règlement (UE) 2016/679. »

10 Protocole n°7 à la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, article 4, CEDH, *Sergueï Zolotoukhine*, paragraphe n° 110. Le droit de l'Union européenne connaît un principe en tout point équivalent reconnu à l'article 50 de la Charte des droits fondamentaux de l'Union européenne, voir notamment CJUE, arrêts du 20 mars 2018, C-524/15, *Luca Menci*, C-537/16, *Garlsson Real Estate SA e.a./Commissione Nazionale per le Società e la Borsa (Consob)*, et C-596/16 et C 597/16 (aff. jointes), *Enzo Di Puma/Consob et Consob/Antonio Zecca*. Cf. Arnaud Lobry, « De la 'convergence' des jurisprudences de la CJUE et de la Cour EDH : l'élaboration d'une définition commune du principe *ne bis in idem* », Geneva Jean Monnet Working Paper n° 25/2016.

qualifications juridiques dont ils sont susceptibles de faire l'objet, pourvu que les poursuites et les sanctions considérées revêtent un caractère pénal[11]. Il renvoie sur cette question à la jurisprudence de la Cour européenne des droits de l'homme, et plus spécifiquement à son arrêt A. et B. c. Norvège[12].

Point 4°

Au sujet de l'article 5*bis*, paragraphe 1er, alinéa 3, il est renvoyé aux observations formulées à l'article 1er, point 1°, en ce qui concerne le cadrage normatif insuffisant du pouvoir du Grand-Duc dans une matière réservée à la loi. Partant, le Conseil d'État s'oppose formellement à la disposition sous examen pour les motifs figurant à l'endroit de la disposition précitée.

Au paragraphe 2, alinéa 2, il s'impose, sous peine d'opposition formelle pour non-respect de la Constitution, de viser un « règlement grand-ducal » au lieu d'un « arrêté grand-ducal », étant donné qu'il s'agit d'une mesure d'exécution générale que le législateur confie au Grand-Duc en exécution de l'article 45 de la Constitution.

Les paragraphes 3 et 4 n'appellent pas d'observation.

Pour ce qui est du paragraphe 5, le Conseil d'État renvoie à ses observations relatives au point 3°.

Point 5°

Le Conseil d'État renvoie à ses considérations relatives au paragraphe 2 du nouvel article 24-3 du Code de procédure pénale et propose de reformuler la disposition sous examen comme suit :

> « […] à l'exception des données qui ont fait l'objet d'une des mesures prévues à l'article 48-27 du Code de procédure pénale. »

Points 6° et 7°

Sans observation.

Point 8°

Pour ce qui est du paragraphe 5, le Conseil d'État renvoie à ses observations relatives au point 3°.

Point 9°

Pour ce qui est du paragraphe 3, le Conseil d'État renvoie à ses observations relatives au point 3°.

Article 3

Point 1°

Sans observation.

Point 2°

Les paragraphes 1er à 3, 5 et 6, n'appellent pas d'observation.

En ce qui concerne le paragraphe 4, alinéa 1er, il est renvoyé aux observations formulées à l'article 1er, point 1°, à l'article 24-3, paragraphe 1er, alinéa 3, lettre c), et à l'opposition formelle y formulée qui est réitérée.

Point 3°

Sans observation.

Articles 4 et 5

Sans observation.

---

11 Avis du Conseil d'État n° 52.971 du 22 janvier 2019 sur le projet de loi 1° relative aux prospectus pour valeurs mobilières ; 2° portant mise en œuvre du règlement (UE) 2017/1129 du Parlement européen et du Conseil du 14 juin 2017 concernant le prospectus à publier en cas d'offre au public de valeurs mobilières ou en vue de l'admission de valeurs mobilières à la négociation sur un marché réglementé, et abrogeant la directive 2003/71/CE (doc. parl. n° 7328[2], p. 10).

12 CEDH, GC, *A. et B. c. Norvège*, arrêt du 15 novembre 2016, concernant la condamnation de deux contribuables à une sanction fiscale (majoration d'impôts) et à une sanction pénale (peine d'emprisonnement).

Article 6

Pour ce qui est de l'alinéa 1er, le Conseil d'État ne voit pas l'utilité de déroger aux règles de droit commun en matière de publication et d'entrée en vigueur prévues à l'article 4 de la loi du 23 décembre 2016 concernant le Journal officiel du Grand-Duché de Luxembourg, d'autant plus que la formule employée par les auteurs peut conduire à une réduction du délai de quatre jours de droit commun, dans l'hypothèse où la publication a lieu vers la fin du mois. Si les auteurs souhaitent néanmoins prévoir une entrée en vigueur au premier jour du mois, le Conseil d'État recommande soit de veiller à ce que la publication de l'acte en projet se fasse au moins quatre jours avant la date de l'entrée en vigueur souhaitée, soit de prévoir la mise en vigueur le premier jour du deuxième mois qui suit celui de sa publication au Journal officiel du Grand-Duché de Luxembourg.

*

OBSERVATIONS D'ORDRE LEGISTIQUE

Observation préliminaire

Le Conseil d'État signale que lorsqu'un projet de loi comporte des modifications de plusieurs actes et si le nombre des modifications y relatives s'avère trop important, il est indiqué de regrouper les modifications relatives à un même acte sous un chapitre distinct, tout en reprenant chaque modification sous un article particulier.

L'intitulé complet ou, le cas échéant, abrégé de l'acte à modifier doit obligatoirement être mentionné au dispositif à la première modification qu'il s'agit d'apporter à cet acte, même s'il a déjà été cité à l'intitulé ou auparavant au dispositif. Les modifications subséquentes que le dispositif apporte à cet acte se limiteront à indiquer « du même code » ou « de la même loi », en lieu et place de la citation de l'intitulé.

En raison de ce qui précède, le projet de loi sous avis est à restructurer comme suit :

« Chapitre 1er – Modification du Code de procédure pénale

Art. 1er. À 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. […]. »

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

« Art. 48-27. […]. »

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

« Art. 67-1. […]. »

Chapitre 2 – Modification de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques

Art. 4. 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, il est rétabli une lettre (b), libellée comme suit :

« (b) […] ; ».

Art. 5. […].

Art. 6. […].

Art. 7. […].

Art. 8. […].

Art. 9. L'article 7, paragraphe 5*bis*, de la même loi, est remplacé comme suit :

« (5*bis*) […]. »

Art. 10. […].

Art. 11. […].

Art. 12. […].

Chapitre 3 – Modification de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat

Art. 13. […].

Art. 14. À la suite de l'article 7 de la même loi sont insérés les articles 7-1 et 7-2 nouveaux, libellés comme suit :

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

[…].

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

[…]. »

Chapitre 4 – Dispositions finales

Art. 15. […].

[…]. »

Observation générale

Lors des renvois, les différents éléments auxquels il est renvoyé sont à séparer par des virgules, en écrivant, à titre d'exemple à l'article 2, point 2°, phrase liminaire, « L'article 3, paragraphe 1er, alinéa 2, de la même loi, ».

Intitulé

L'intitulé du projet de loi sous avis prête à croire que le texte de loi en projet comporte tant des dispositions autonomes que des dispositions modificatives. Comme la visée de la loi en projet est toutefois entièrement modificative, il y a lieu de reformuler l'intitulé de manière qu'il reflète cette portée.

Aux énumérations, le terme « et » est à omettre à l'avant-dernier élément comme étant superfétatoire. Cette observation vaut également pour l'article 2, point 2°, à l'article 3, paragraphe 1er, alinéa 2, deuxième tiret.

En raison de ce qui précède, l'intitulé de la loi en projet est à reformuler comme suit :

« Projet de loi 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 ;

3° de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État ».

Article 1er

Au point 1°, à l'article 24-3, paragraphe 1er, alinéa 3, il est signalé qu'au sein des énumérations, chaque élément commence par une minuscule. Cette observation vaut également pour l'article 2, point 4°, à l'article 5*bis*, paragraphe 2, alinéa 1er.

Au point 3°, à l'article 67-1, paragraphe 1er, alinéa 1er, phrase liminaire, il est signalé que le recours à la forme « et/ou », que l'on peut généralement remplacer par « ou », est à éviter. Cette observation vaut également pour l'article 3, point 3°, à l'article 7-2, paragraphe 2, point 2°. À l'alinéa 2, le Conseil d'État précise que lorsqu'on se réfère au premier alinéa, les lettres « er » sont à insérer en exposant derrière le numéro pour écrire « 1er ». Cette observation vaut également pour le paragraphe 3, alinéa 1er, deuxième phrase. Au paragraphe 3, il est signalé que les nombres s'écrivent en toutes lettres, qu'ils s'expriment uniquement en chiffres s'il s'agit de pour cent, de sommes d'argent, d'unités de mesure,

d'indices de prix ou de dates. Cette observation vaut également pour l'article 2, points 3°, à l'article 5, paragraphe 2, deuxième phrase, et 7°, à l'article 7, paragraphe 5*bis*, deuxième phrase.

Article 2

Au point 1°, phrase liminaire, il convient de viser la « lettre (b) » et non le « point (b) ». Par ailleurs, le Conseil d'État signale que la formule « il est rétabli une lettre X » est à retenir lorsque, par suite d'une abrogation antérieure, le numéro de lettre est vacant et qu'on le réutilise.

Au point 2°, à l'article 3, paragraphe 1er, alinéa 2, phrase liminaire, il est signalé que lorsqu'un acte est cité, il faut veiller à reproduire son intitulé tel que publié officiellement, indépendamment de sa longueur. Par ailleurs, au cas où un règlement européen a déjà fait l'objet de modifications, il convient d'insérer les termes « , tel que modifié » après l'intitulé. Tenant compte de ce qui précède, il y a lieu de viser 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), tel que modifié ». En outre, au sein des énumérations, chaque élément se termine par un point-virgule. Cette observation vaut également pour le point 6°, à l'article 5*quater,* paragraphe 1er, alinéa 2.

Au point 3°, à l'article 5, paragraphe 5, première phrase, il est signalé que les références aux dispositions figurant dans le dispositif se font en principe sans rappeler qu'il s'agit du « présent » article. Partant, les termes « du présent article » sont à supprimer.

Étant donné que les points 5° et 6° visent à remplacer des dispositions qui se suivent, ils peuvent être regroupés. Il est renvoyé à la proposition de restructuration ci-dessus.

Au point 6°, à l'article 5*quater,* paragraphe 1er, alinéa 2, phrase liminaire, il convient de se référer à la « Commission nationale pour la protection des données ».

Au point 8°, à l'article 9, paragraphe 1er, le soulignement entre les termes « par le comité ministériel du renseignement pour » et les termes « le Service de renseignement de l'État » est à écarter.

Au point 9°, à l'article 10*ter*, paragraphe 1er, alinéa 1er, point 1°, les termes « de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques » sont à supprimer pour être superfétatoires.

Article 3

Au point 1°, le Conseil d'État comprend à la lecture du texte coordonné de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État joint au projet de loi sous avis, que la modification en question est à apporter à l'article 7, paragraphe 2, alinéa 1er, de la loi précitée du 5 juillet 2016, de sorte qu'il y a lieu d'adapter la disposition en ce sens. Par ailleurs, il y a lieu d'indiquer avec précision et de manière correcte les textes auxquels il est renvoyé, en commençant par l'article et ensuite, dans l'ordre, le paragraphe, l'alinéa, le point, la lettre et la phrase visés. En outre, le Conseil d'État comprend à l'aide dudit texte coordonné que les auteurs souhaitent remplacer le terme « télécommunications » par les termes « communications électroniques » à une reprise uniquement en fin de phrase, de sorte qu'il y a lieu de le préciser.

Les points 2° et 3° peuvent être regroupés. Le Conseil d'État renvoie à sa proposition de restructuration de la loi en projet dans le cadre de ses observations préliminaires.

Article 4

Les termes « celui de » sont à ajouter après les termes « qui suit ».

Article 5

Le Conseil d'État se doit de signaler que l'introduction d'un intitulé de citation est inutile pour un acte à caractère exclusivement modificatif, étant donné qu'un tel acte n'existe pas à titre autonome dans l'ordonnancement juridique et que partant aucune référence n'est censée y être faite dans les autres textes normatifs. Partant, l'article sous examen est à supprimer.

Article 6

En ce qui concerne l'alinéa 1er, il convient d'ajouter les termes « qui suit celui » à la suite des termes « le quatrième jour ».

À l'alinéa 2, les termes « Par dérogation au paragraphe 1er, » sont à supprimer. Subsidiairement, il convient de viser l'« alinéa 1er » et non le « paragraphe 1er ».

Il convient d'écrire « du douzième mois qui suit celui de sa publication ~~de la présente loi~~ au Journal officiel du Grand-Duché de Luxembourg. »

Ainsi délibéré en séance plénière et adopté à l'unanimité des 19 votants, le 23 janvier 2024.

Le Secrétaire général,
Marc BESCH

Le Président,
Christophe SCHILTZ

Impression: CTIE – Division Imprimés et Fournitures de bureau