Session ordinaire 2022-2023

CL/LW P.V. J 18

Commission de la Justice

Procès-verbal de la réunion du 25 janvier 2023

Ordre du jour :

1. 8051 **Projet de loi portant :**
1° modification du Code de procédure pénale;
2° modification de la loi du 17 mars 2004 relative au mandat d'arrêt européen et aux procédures de remise entre Etats membres de l'Union européenne

- Désignation d'un rapporteur
- Présentation et examen des articles
- Echange de vues

2. **Avant-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.

- Présentation et examen des articles
- Echange de vues

3. **Divers**

*

Présents : Mme Diane Adehm, M. Guy Arendt, M. François Benoy, M. Dan Biancalana, Mme Stéphanie Empain, M. Léon Gloden, M. Marc Goergen, Mme Carole Hartmann, M. Pim Knaff, M. Charles Margue, Mme Elisabeth Margue remplaçant Mme Octavie Modert, M. Laurent Mosar, M. Gilles Roth

Mme Sam Tanson, Ministre de la Justice

M. Sven Clement, observateur

M. Gil Goebbels, Mme Christine Goy, Mme Michèle Schummer, M. Laurent Thyes, du Ministère de la Justice

Mme Liz Reitz, attachée parlementaire (déi gréng)

M. Christophe Li, de l'Administration parlementaire

Excusés : Mme Cécile Hemmen, Mme Octavie Modert, M. Roy Reding

Mme Nathalie Oberweis, observateur délégué

*

Présidence : M. Charles Margue, Président de la Commission

1. 8051 Projet de loi portant :
1° modification du Code de procédure pénale;
2° modification de la loi du 17 mars 2004 relative au mandat d'arrêt européen et aux procédures de remise entre Etats membres de l'Union européenne

- Désignation d'un rapporteur
- Présentation et examen des articles
- Echange de vues

Ce point a été reporté à une date ultérieure.

*

2. Avant-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.

- Présentation et examen des articles
- Echange de vues

Remarques préliminaires :

La Commission de la Justice entend désigner Mme Stéphanie Empain (déi gréng) comme rapportrice de l'avant-projet de loi sous rubrique.

Mme Sam Tanson (Ministre de la Justice, déi gréng) renvoie au contexte juridique actuel qui encadre la rétention des données dans le secteur des communications électroniques et qui est issu du droit européen dérivé. L'oratrice souligne la nécessité de conformer la législation nationale aux différents arrêts[1] de la Cour de justice de l'Union européenne (ci-après « CJUE

[1] Il convient de se référer aux arrêts suivants :

»). Il s'agit de garantir un juste équilibre entre le droit à la vie privée et la nécessité de créer un cadre légal adéquat en matière de lutte contre la criminalité grave.

Au niveau du conseil européen, les négociations entre les Etats membres n'ont pas avancé significativement, et ce, en raison de la divergence des opinions existantes en matière de la rétention des données entre les différents Etats membres.

A noter que le projet de loi n° 6763[2], qui a été déposé le 7 janvier 2015 par M. le Ministre de la Justice de l'époque, ne tient pas compte des dernières évolutions jurisprudentielles de la CJUE.

L'expert gouvernemental explique les choix opérés par les auteurs de la future loi sur la structure de celle-ci et liste les différentes données à caractère personnel qui peuvent faire l'objet d'une telle conservation. Quant à l'accès, il y a lieu de signaler que les modalités légales restent inchangées et sont régies déjà par les lois en vigueur, à savoir le Code de procédure pénale et la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat.

Une autre innovation constitue la terminologie employée au sein de la future loi, alors que des plateformes de messageries instantanées sont désormais visées par celle-ci. Cette adaptation de la terminologie fait suite à une réforme européenne qui a été transposée par le législateur en droit national au cours de l'année 2021.

Présentation de l'avant-projet de loi et examen des articles

Article 1er de l'avant-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*

- CJUE, 8 avril 2014, Digital Rights Ireland et Seitlinger, affaires jointes C293/12 et C594/12 ;
- CJUE, 21 décembre 2016, Tele2 Sverige AB (C-203/15) et Secretary of State for the Home Department, affaire C-698/15 ;
- 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) ;
- CJUE, 5 avril 2022, G.D. contre Commissioner of An Garda Síochána, affaire C-140/20 ; 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.

[2] Projet de loi 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

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 10ter, 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 10ter, paragraphe 2, de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques à l'identification de l'utilisateur d'une adresse IP.

(3) Lorsqu'il existe une nécessité urgente de prévenir une atteinte grave à la vie, à la liberté ou à l'intégrité physique d'une personne ou lorsqu'il est impératif que les autorités qui procèdent à l'enquête agissent immédiatement pour éviter de compromettre sérieusement une procédure pénale, les officiers de police judiciaire visés à l'article 10 peuvent, avec l'accord oral et préalable du procureur d'État ou du juge d'instruction, et par une décision motivée et écrite requérir 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 324quater 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. »

Commentaire de l'article 1er (modification du Code de procédure pénale)

Dans ses arrêts du 6 octobre 2020[3] et du 5 avril 2022[4], 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[5]. 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 (…)* »[6].

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*

[3] CJUE, 6 octobre 2020, Privacy international (affaire C-623/17), et La Quadrature du Net, French Data Network, Ordre des barreaux francophones et germanophones (affaires jointes C-511/18, C-512/18, C-520-18).
[4] CJUE, 5 avril 2022, G.D. contre Commissioner of An Garda Síochána, affaire C-140/20.
[5] Paragraphes 140 et suivants de l'arrêt du 6 octobre 2020.
[6] Paragraphe 148 de l'arrêt du 6 octobre 2020.

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 » [7].

Par conséquent, l'article 1er, point 1°, du projet de loi propose d'introduire un nouvel article 24-3 dans le 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 communications 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.

[7] Paragraphe 78 de l'arrêt du 5 avril 2022.

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 inspiré 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 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 messageries 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 de l'avant-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* dans 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°, de l'avant-projet de loi.

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

Par analogie à cette modification terminologique, l'avant-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 à la 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 avant-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[8]. 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 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, 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*[9] ».

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[10] concernant le projet de loi n° 6763 que « *[c]ette solution, retenue dès l'insertion de l'article 67-1 au Code*

[8] CJUE, 8 avril 2014, Digital Rights Ireland et Seitlinger e.a. (affaires jointes C-293/12 et C-594/12).
[9] Paragraphe 109 de l'arrêt du 5 avril 2022.
[10] Document parlementaire n° 6763[3].

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 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. L'avant-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[11], « *[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 l'avant-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°, de l'avant-projet de loi susmentionné.

Article 2 de l'avant-projet de loi

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:*

[11] Page 58 du document parlementaire n° 2572/001.

- *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. 5bis. (1) Pour les besoins de sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention de menaces graves contre la sécurité publique, tout fournisseur d'un service de communications électroniques ou opérateur est tenu de conserver les données relatives au trafic et à la localisation pour les zones géographiques visées au paragraphe 2, pendant six mois à partir de la date de la communication.*
L'obligation de conserver inclut la conservation des données relatives aux appels téléphoniques infructueux lorsque ces données sont générées ou traitées et stockées, en ce qui concerne les données de la téléphonie, ou journalisées, en ce qui concerne les données de l'internet, dans le cadre de la fourniture des services de communications concernés. Pour l'application du présent paragraphe, une seule information de localisation est requise par communication ou appel.

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

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

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

a) Les lieux où sont commis, de manière répétée, des crimes ou délits dont les faits emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement ;
b) Les lieux qui par leur configuration sont de nature à favoriser la commission des crimes ou délits dont les faits emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement ;
c) Les alentours et abords des infrastructures où sont organisés régulièrement des 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. 5ter. (1) Les données conservées au titre des articles 5, 5bis et 9 de la présente loi par les autorités compétentes au sens de l'article 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. 5quater. (1) La Commission nationale pour la protection des données publie annuellement des statistiques sur la conservation de données au titre des articles 5 et 9.*
A cet effet les fournisseurs de services de communications électroniques ou opérateurs conservent et continuent à la Commission nationale, sur demande de celle-ci, les informations comprenant notamment:

- *les cas dans lesquels des informations ont été transmises aux autorités compétentes conformément à la législation nationale applicable,*

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

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

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

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

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

« *Art. 9. Données de localisation autres que les données relatives au trafic*
(1) Tout fournisseur de services de communications électroniques ou opérateur qui traite des données de localisation, autres que les données relatives au trafic, concernant les abonnés et les utilisateurs, est tenu de prendre toutes les dispositions nécessaires à ce que de telles données soient effacées ou rendues anonymes dès lors qu'elles ne sont plus nécessaires à la transmission d'une communication ou aux traitements prévus par les dispositions des paragraphes 2 et 3, à l'exception des accès qui sont ordonnés par les autorités judiciaires et par le comité ministériel du renseignement pour le Service de renseignement de l'Etat agissant dans le cadre des compétences leur attribuées par la loi pour sauvegarder la sécurité nationale, pour la lutte contre la criminalité grave et pour la prévention de menaces graves contre la sécurité publique.

(2) Tout fournisseur de services concernés ou opérateur ne peut traiter des données de localisation autres que les données relatives au trafic et concernant les abonnés ou les utilisateurs que si celles-ci ont été rendues anonymes ou moyennant le consentement de l'abonné ou de l'utilisateur, dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée et sous réserve des dispositions des paragraphes 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. 10ter. Conservation des données d'identification*
(1) Tout fournisseur d'un service de communications électroniques ou opérateur est tenu de conserver les données suivantes, pour autant qu'il les traite ou les génère dans le cadre de la fourniture de ses services :

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

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

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

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

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

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

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

L'opérateur ou le fournisseur des services concernés conserve les données visées à l'alinéa 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. »

Commentaire de l'article 2 de l'avant-projet de loi (modification 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 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 »).

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

Dans son arrêt « Digital Rights Ireland » de 2014, la CJUE a invalidé la directive sur la conservation des données[12] 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[13], 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°, de l'avant-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.

[12] 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).
[13] CJUE, 21 décembre 2016, Tele2 (affaires C-203/15 et C-698/15).

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[14].

L'avant-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 avant-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 de l'avant-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 de l'avant-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°, de l'avant-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 de l'avant-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.
L'avant-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*

[14] 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*. »

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 avant-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* »[15].
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* »[16].
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°, de l'avant-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.

[15] Paragraphe 146 de l'arrêt du 6 octobre 2020.
[16] 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* »[17].
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* » et 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, les capacités rapides d'adaptation des criminels et les différents facteurs d'émergence des crimes, l'avant-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

[17] Paragraphe 150 de l'arrêt du 6 octobre 2020.

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.

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 à la 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.* »[18]
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 à l'article 2, point 3°, de l'avant-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°, de l'avant-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.

[18] Paragraphe 82 de l'arrêt du 5 avril 2022.

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 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, l'avant-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°, de l'avant-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°, de l'avant-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 soit 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 »*[19].

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.

[19] Paragraphes 157, 158 et 159 de l'arrêt du 6 octobre 2020.

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

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

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

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

L'IMEI est un numéro d'identification unique qui permet d'immatriculer un équipement mobile. L'IMEI constitue une donnée essentielle à l'identification de l'auteur présumé d'une infraction. En pratique, on observe que, surtout dans des affaires de stupéfiants, les auteurs d'infractions changent de cartes SIM et les placent dans un seul et même appareil pour communiquer. Le numéro IMEI de l'équipement terminal est ainsi indispensable dans le cadre de l'enquête ou de l'instruction.
Puis, si une certaine carte SIM est enregistrée sous un faux nom, mais qu'elle est utilisée dans un appareil auquel peut être associée une seconde carte SIM dont le titulaire est correctement identifié, cela donne une indication sur la véritable identité de l'utilisateur de la première carte SIM.

Il échet de noter dans ce contexte que l'IMSI et l'IMEI ne permettent donc pas le traçage du parcours de navigation d'un utilisateur, qui serait couvert par la mesure de repérage, mais elles servent 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°, de l'avant-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. Elle sert principalement à identifier, par l'intermédiaire des fournisseurs concernés, la personne physique propriétaire d'un équipement terminal à partir duquel une communication au moyen de l'Internet est effectuée, telle qu'autorisée 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. »[20]
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. »[21]
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 :

[20] Paragraphe 159 de l'arrêt du 6 octobre 2020.
[21] Paragraphe 159 de l'arrêt du 6 octobre 2020.

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.

Article 3 de l'avant-projet de loi (modifications de la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'Etat)

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. »

Commentaire

L'article 3, point 1°, de l'avant-projet de loi adapte la définition des opérateurs et fournisseurs concernés à la lumière des autres dispositions proposées par le présent avant-projet de loi et il est renvoyé aux explications données sous l'article 1er, point 1°, de l'avant-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 (dénommée ci-après 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 communications 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 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*[22] ».
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* [23] ».
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*

[22] Paragraphe 48 de l'arrêt du 5 avril 2022.
[23] Paragraphe 136 de l'arrêt du 6 octobre 2020.

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[24] ».

L'article 3, point 2°, de l'avant-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*[25] ». 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* » [26].

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°, de l'avant-projet de loi et il est dès lors renvoyé aux explications fournies pour ladite disposition.

<u>Article 4 de l'avant-projet de loi (disposition transitoire) :</u>

[24] Paragraphe 137 de l'arrêt du 6 octobre 2020.
[25] Paragraphe 138 de l'arrêt du 6 octobre 2020.
[26] Paragraphe 139 de l'arrêt du 6 octobre 2020.

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.

Commentaire

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°, de l'avant-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.

L'article 4 de l'avant-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 de l'avant-projet de loi (intitulé de l'avant-projet de loi) :

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. »

Commentaire

L'article 5 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 de l'avant-projet de loi – entrée en vigueur :

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°, entre en vigueur le premier jour du douzième mois qui suit la publication de la présente loi au Journal officiel du Grand-Duché de Luxembourg.

Commentaire

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 de l'avant-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.

Echange de vues

M. Marc Goergen (Piraten) souhaite avoir des informations supplémentaires sur la mise en application de la future loi en cas de recours par un utilisateur à un réseau wifi qui est publiquement accessible.

Un autre point qui suscite des interrogations constitue le recours aux connexions à internet à l'aide d'un outil VPN. De plus, l'orateur est d'avis que le recours à l'utilisation des cartes SIM du type « *e-SIM* » achetées dans un pays tiers risque de remettre en cause le bon fonctionnement de la future loi.

Enfin, l'orateur critique le fait que des opérateurs de télécommunications sont actuellement obligés de conserver des données personnelles des utilisateurs de manière indifférenciée, alors que des appels téléphoniques entre des mandants et leurs avocats tombent sous le régime de la conservation des données et que ceux-ci sont *a priori* couverts par le secret professionnel. Cette même critique vaut également pour la protection des sources journalistiques qui ne peut être garantie de manière satisfaisante en cas de conservation généralisée de données de télécommunication des utilisateurs.

Mme Sam Tanson (Ministre de la Justice, déi gréng) juge utile de rappeler la finalité du présent avant-projet de loi et indique que celui-ci constitue une avancée considérable en matière de la protection des données et entend à garantir que le droit luxembourgeois soit conforme à la jurisprudence de la CJUE qui a invalidé l'obligation générale de conservation des données relatives au trafic et des données de localisation imposée par la directive européenne 2006/24/EC.

L'oratrice indique que la protection des sources journalistiques et le secret professionnel des avocats ne sont pas remis en cause par le présent avant-projet de loi. Ces principes sont garantis comme ils sont inscrits dans les lois nationales.

Quant à l'usage des outils de VPN, susceptibles de masquer les adresses IP, ou encore le fait que des cartes SIM peuvent être achetées dans des pays hors de l'Union européenne et utilisées au Luxembourg, il y a lieu de signaler que le droit luxembourgeois s'applique uniquement sur le territoire national. Aucun changement de paradigme n'est opéré par le présent avant-projet de loi en la matière et si les autorités judiciaires souhaitent, dans le cadre d'une enquête pénale, avoir des informations sur l'identité de l'acheteur d'une carte SIM, qui a été achetée dans un pays tiers, elles devront recourir aux outils de la coopération judiciaire internationale existants, comme cela peut se faire déjà à l'heure actuelle.

M. Laurent Mosar (CSV) est d'avis que le présent avant-projet de loi est particulièrement important au regard du droit de la protection des données et signale également que le cadre légal à créer en la matière est hautement complexe. L'orateur souhaite avoir davantage d'informations sur les droits des usagers et savoir si ces derniers ont la faculté d'obtenir des renseignements auprès des opérateurs de télécommunications sur l'ampleur des données qui sont collectées sur eux.

Un autre point qui suscite des interrogations de l'orateur constitue l'accès aux données collectées par des différents opérateurs téléphoniques. Il souligne l'importance d'une réglementation stricte en la matière, afin d'éviter que des employés des opérateurs pourraient,

sans raison légitime, accéder au contenu de ces données et espionner les clients de cet opérateur.

Par ailleurs, l'orateur souhaite avoir des informations sur l'identification des données personnelles des usagers et celle des numéros téléphoniques composés par les usagers.

Enfin, l'orateur se demande si les cartes de crédit tombent sous le champ de la future loi, alors qu'à l'aide de l'historique des paiements effectués par les usagers, il est possible de prendre connaissance des aspects intimes de la vie privée des usagers par ce moyen de paiement.

Mme Sam Tanson (Ministre de la Justice, déi gréng) indique qu'il y a lieu de distinguer clairement entre, d'une part, le droit commun du droit de la protection des données qui garantit aux consommateurs et clients d'entreprises commerciales une protection contre une ingérence injustifiée dans leur vie privée de la part des opérateurs économiques et, d'autre part, les dispositions de la future loi, qui elles règlent la conservation par des opérateurs de télécommunications des données à caractère personnel des utilisateurs, et ce, dans une optique de constatation et de la poursuite d'infractions pénales. Ainsi, l'accès à ces données conservées par les autorités judiciaires est soumis à des règles strictes et ces dispositions ne sont pas modifiées par le biais du présent avant-projet de loi.

A noter que si les Députés entendent discuter du régime de droit commun applicable à la protection des données et des dispositions applicables aux sociétés commerciales qui proposent des services de télécommunications ou qui sont émettrices de cartes de crédit, il convient de mener cette discussion avec le ministre de ressort compétent.

L'expert gouvernemental précise qu'il y a lieu de distinguer entre, d'une part, les données conservées et, d'autre part, l'accès à ces données par les autorités judiciaires. Ainsi, une conservation de données qui est faite par les opérateurs de télécommunications ne confère pas aux autorités judiciaires un accès automatique à ces données. Ici, les conditions légales imposées par le Code de procédure pénale doivent être remplies et l'enquête effectuée devra viser des infractions relevant de la criminalité grave, avant qu'un accès aux données conservées ne puisse être conféré aux autorités judiciaires.

Quant aux données d'identification collectées, il y a lieu de préciser que celles-ci servent aux opérateurs de télécommunications, et en cas d'accès conféré aux autorités judiciaires dans une enquête pénale, d'identifier les utilisateurs. Ces données d'identification ne permettent cependant pas aux opérateurs de télécommunications d'effectuer une écoute des télécommunications effectuées ou un traçage des habitudes des utilisateurs. Une réponse similaire s'impose au cas où une carte de crédit est utilisée par un client qui recourt à des services de télécommunications, comme le numéro de cette carte bancaire permet uniquement une identification de celui-ci, sans pour autant donner automatiquement aux autorités judiciaires un accès à l'historique des paiements effectués par le biais de ce moyen de paiement électronique.

M. Sven Clement (Piraten) appuie le fait qu'un avant-projet de loi portant réforme du régime applicable à la conservation des données soit présenté par le Gouvernement, alors qu'une panoplie d'arrêts jurisprudentiels existe entretemps. Cependant, plusieurs observations critiques sont à soulever à l'encontre du texte proposé. De prime abord, l'orateur est d'avis que plusieurs dispositions manquent de précision et risquent d'induire en erreur les citoyens sur les zones géographiques dans lesquelles des données de télécommunication seront conservées dans le futur. L'orateur cite l'exemple d'un stade de football et d'une salle de concerts qui sont susceptibles d'accueillir plusieurs milliers de spectateurs. L'orateur estime que dans ces édifices et des alentours, une conservation indifférenciée des données de télécommunication sera effectuée sans que cela soit précisé expressément dans le texte de la future loi.

L'orateur renvoie à la législation allemande, qui permet une conservation généralisée et indifférenciée des données de télécommunication dans des zones regroupant un grand nombre de personnes (communément appelé « *Rasterfahndung* »). Ainsi, il est régulièrement critiqué par des membres de la société civile allemande que cette disposition sert aux autorités publiques de procéder à une conservation généralisée et indifférenciée des données de télécommunication des manifestants qui protestent contre la politique gouvernementale.

L'orateur renvoie par la suite aux protocoles informatiques qui s'appliquent dans le cadre de la connexion d'un appareil électronique à un réseau internet, et exprime son inquiétude que de nombreuses données seront conservées, sans que cela soit nécessaire. A titre d'exemple, l'orateur renvoie à certaines législations étrangères qui imposent la conservation des adresses Mac, en raison des spécificités applicables aux ordinateurs de la marque *Apple*.

En outre, l'orateur exprime sa crainte que la future législation rendra impossible la mise à disposition de wifi publics. Il renvoie à l'article 2, point 10°, de l'avant-projet de loi qui oblige les fournisseurs d'un service de communications électroniques de conserver un certain nombre de données, pour autant qu'il les traite ou les génère dans le cadre de la fourniture de ses services.

Enfin, l'orateur regarde d'un œil critique le fait que parmi les conditions d'accès aux données stockées, un seuil de peines d'une année d'emprisonnement a été mis en place dans la future loi. L'orateur signale que le Code pénal prévoit un nombre considérable d'infractions qui ne sont pas nécessairement à considérer comme relevant de la criminalité grave mais qui sont tout de même susceptibles de tomber dans le champ d'application de la future loi, comme ces infractions peuvent être sanctionnées par une peine d'emprisonnement égale ou supérieure à un an.

Mme Sam Tanson (Ministre de la Justice, déi gréng) ne partage pas le point de vue de M. Sven Clement (Piraten) quant au risque de disparition de wifi publics en raison de la future loi. L'oratrice signale que le libellé énonce, comme condition de conservation de certaines données, que celles-ci soient traitées ou générées par cet opérateur ce qui n'est nécessairement pas le cas d'un opérateur qui met à disposition des tiers un wifi. De plus, il y a lieu de relever que l'élaboration de la réglementation applicable aux wifi publics ne relève pas du champ de compétence du ministre de la Justice.

L'expert gouvernemental renvoie au concept de la « *Rasterfahndung* » et explique que la législation luxembourgeoise en matière d'accès aux données à caractère personnel diffère de celle applicable en Allemagne, de sorte qu'on ne saurait raisonner par analogie sur ce point.

Quant aux adresses Mac, l'expert précise que la loi belge en la matière prévoit en effet une conservation de ces données. Or, la législation luxembourgeoise ne liste pas ces adresses Mac étant donné que celles-ci ne sont pas toujours disponibles.

Mme Sam Tanson (Ministre de la Justice, déi gréng) précise que le libellé retenu par les auteurs de l'avant-projet de loi est une reprise fidèle de la jurisprudence de la CJUE et vise à conformer la législation luxembourgeoise aux exigences du droit européen.
Quant au seuil de peine d'un an d'emprisonnement, il convient de noter que ceci a fait en amont l'objet d'une longue discussion sur les avantages et désavantages parmi les auteurs de l'avant-projet de loi. Au fil du temps, des infractions nouvelles et des ajustements de sanctions d'infractions existantes ont été insérés dans le Code pénal luxembourgeois. Force est de constater que ces changements reflètent, dans une certaine manière, les évolutions sociétales des décennies dans lesquelles ces réformes législatives ont été adoptées. Cependant, il convient aujourd'hui de dresser le constat que ceci n'a pas été bénéfique pour la cohérence des textes de loi regroupés dans ce code et qu'il comporte de nombreuses infractions et

sanctions qui ne reflètent plus les mœurs actuelles, alors que d'autres infractions, qui sont de nos jours considérées comme graves, ne sont pas sévèrement sanctionnées par ce code. Un groupe de travail examine les dispositions contenues dans ce code, ce qui constitue un travail complexe et de longue haleine.

M. Charles Margue (Président, déi gréng) salue le fait qu'un premier échange de vues sur la future loi a eu lieu lors de la réunion de ce jour, tout en rappelant le fait que l'instruction parlementaire ne vient que de démarrer et que dans les semaines et mois à venir, de nombreux avis consultatifs seront soumis au Parlement et qui vont certainement donner des impulsions additionnelles sur cet avant-projet de loi important.

*

3. Divers

M. Charles Margue (Président, déi gréng) informe les membres de la commission parlementaire qu'une entrevue avec Mme Diane Schmitt, coordinatrice européenne de la lutte contre la traite des êtres humains, aura lieu le 24 mars 2023.

*

Procès-verbal approuvé et certifié exact