N° 8148²

CHAMBRE DES DEPUTES

Session ordinaire 2022-2023

PROJET DE LOI

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

1° du Code de procédure pénale ;

2° de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques ; et

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

* * *

AVIS DU PARQUET GENERAL

(13.3.2023)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

L'injonction aux fournisseurs de services de communications électroniques de conserver de manière généralisée et indifférenciée des données relatives au trafic et à la localisation doit faire l'objet d'un contrôle effectif, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant afin de vérifier l'existence de l'une des situations de menace envisagées ainsi que le respect des conditions et des garanties prévues.

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

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

---

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

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

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

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

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

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

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

La conservation ciblée, temporellement limitée au strict nécessaire, des données relatives au trafic et à la localisation, qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, voire d'autres critères objectifs, doit par ailleurs faire l'objet d'un contrôle effectif, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, afin de vérifier l'existence d'une de ces situations ainsi que le respect des conditions et des garanties prévues.

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

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

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

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

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

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

---

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

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

*

COMMENTAIRE DES ARTICLES

Article 1er 1°

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

L'article n'envisage pas cette hypothèse.

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

---

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

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

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

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

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

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

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

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

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

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

Article 1er 2°

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

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

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

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

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

---

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

Article 1er 3°

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

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

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

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

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

Article 2 1°

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

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

Article 2 2°

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

Article 2 3°

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

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

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

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

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

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

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

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

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

Article 2 4°

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

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

L'article analysé précise les zones géographiques pour lesquelles les données devront être conservées, à savoir les zones particulièrement exposées à des menaces pour la sécurité nationale ou à des risques élevés de préparation ou de commission d'actes de criminalité grave.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Article 2 5°

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

Article 2 6°

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

Article 2 7°

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

Article 2 8°

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

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

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

Article 2 9°

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

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

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

- Adresses IP ayant servi à la souscription ou à l'activation du service de communication électronique ainsi que le port source de la connexion et l'horodatage ;
- L'identité internationale d'abonné mobile (IMSI) :
- L'identité internationale d'équipement mobile (IMEI).

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

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

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

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

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

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

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

*

Article 3

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

*

Article 4

Cet article prévoit que la commission consultative dont la création est prévue aux termes de paragraphe 4 de l'article 5bis de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques, présentera sa proposition de l'étendue du périmètre de chaque zone géographique au Haut-Commissariat à la protection nationale au plus tard le premier jour du troisième mois qui suit la publication de la loi au Journal officiel du Grand-Duché de Luxembourg.

Suite à la communication de l'arrêté grand-ducal y afférent aux opérateurs et fournisseurs concernés, ces derniers disposeront d'un délai restant de neuf mois afin de prendre les mesures techniques et organisationnelles nécessaires pour procéder à la mise en place de la conservation ciblée et de la suppression des données résiduelles non visées par ladite conservation.

Article 5

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

Article 6

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

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

Luxembourg, le 13 mars 2023

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

Impression: CTIE – Division Imprimés et Fournitures de bureau