N° 8148[3]

CHAMBRE DES DEPUTES

Session ordinaire 2022-2023

PROJET DE LOI

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

1° du Code de procédure pénale ;

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

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

* * *

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

(13.4.2023)

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

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

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

---

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

Ad article 1er du projet de loi

• *Ad nouvel article 24-3 CPP*

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

Soulignons que l'injonction dite « *quick freeze* » porte uniquement sur la conservation des données et non pas sur leur communication aux autorités judiciaires. Tel que le soulignent les auteurs du projet de loi, l'accès se fait dans les conditions prévues par l'article 67-1 CPP. Pourtant, le second alinéa de l'article 24-3 CPP renvoie à un règlement grand-ducal qui détermine les catégories de données pouvant faire l'objet de la mesure de conservation et qui « *peut également déterminer les formes et les modalités suivant lesquelles les données visées sont à mettre à disposition des autorités judiciaires* ». Afin d'assurer la cohérence et lisibilité du texte, il serait opportun, d'une part, de renvoyer explicitement au règlement grand-ducal du 24 juillet 2010 déterminant les catégories de données à caractère personnel générées ou traitées dans le cadre de la fourniture de services de communications électroniques ou de réseaux de communications publics, que les auteurs du projet de loi visent dans leurs commentaires. D'autre part, la dernière phrase du second alinéa de l'article 24-3 CPP concernant l'accès aux données devrait être remplacée par un renvoi à l'article 67-1CPP. C'est d'ailleurs une disposition similaire qui figure au dernier paragraphe de l'article 39*quinquies* du Code d'instruction criminelle (ci-après CIC) belge, dont la disposition sous examen est inspirée[2].

---

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

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

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

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

La décision écrite et motivée mentionne:

- *le nom du procureur du Roi qui ordonne la conservation;*
- *l'infraction qui fait l'objet de l'ordre;*
- *les circonstances de fait de la cause qui justifient la conservation;*
- *l'indication précise d'un ou de plusieurs des éléments suivants: la personne ou les personnes, les moyens de communication ou les lieux qui font l'objet de la conservation;*
- *le cas échéant, les catégories de données de trafic et de localisation qui doivent être conservées;*
- *la durée de la mesure, qui ne peut excéder deux mois à compter de la date de l'ordre, sans préjudice de renouvellement;*
- *la durée de conservation des données, qui ne peut excéder six mois. Ce délai peut être prolongé par écrit.*

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

§ 2. Les acteurs visés au paragraphe 1er, alinéa 2, veillent à ce que l'intégrité, la qualité et la disponibilité des données soit garantie et à ce que les données soient conservées de manière sécurisée.

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

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

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

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

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

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

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

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

• *Ad nouvel article 48-27 CPP*

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

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

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

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

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

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

• *Ad nouvel article 67-1 CPP*

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

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

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

---

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

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

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

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

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

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

---

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

« § 1er S'il existe des indices sérieux que les infractions sont de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde, et lorsque le juge d'instruction estime qu'il existe des circonstances qui rendent le repérage de communications électroniques ou la localisation de l'origine ou de la destination de communications électroniques nécessaire à la manifestation de la vérité, il peut faire procéder:

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

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

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

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

Dans les cas visés à l'alinéa 1er, pour chaque moyen de communication électronique dont [5 les données de trafic]5 sont repérées ou dont l'origine ou la destination de la [5 communication électronique]5 est localisée, le jour, l'heure, la durée et, si nécessaire, le lieu de la communication électronique sont indiqués et consignés dans un procès-verbal. Le juge d'instruction indique les circonstances de fait de la cause qui justifient la mesure, son caractère proportionnel eu égard au respect de la vie privée et subsidiaire à tout autre devoir d'enquête, dans une ordonnance motivée.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Ad article 2 du projet de loi

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

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

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

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

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

Quant aux conditions dans lesquelles la conservation est autorisée, le projet de loi distingue, d'une part, la conservation généralisée des adresses IP prévue par le nouvel article 10*ter* (2) de la loi Telecom et, d'autre part, la conservation ciblé des données relatives au trafic et à la localisation régie par le nouvel article 5*bis* de la loi Telecom. Cette seconde disposition viserait, d'après le commentaire des articles, les métadonnées définies par le règlement grand-ducal du 24 juillet 2010 déterminant les catégories de données à caractère personnel générées ou traitées dans le cadre de la fourniture de services de communications électroniques ou de réseaux de communications publics. Dans un souci de lisibilité, la référence exacte audit règlement pourrait être insérée au troisième alinéa du nouvel article 5*bis* (1) de la loi Telecom.

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

---

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

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

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

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

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

Il résulte toutefois du nouvel article 5*bis* (2), point 1°, lettre a) de la loi Telecom que la conservation ciblée de données relatives au trafic et à la localisation sera notamment possible dans « *les lieux où sont commis, de manière répétée, des crimes ou délits dont les faits emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement* ». Il n'est fait référence à aucun seuil prédéfini, aucune différenciation plus détaillée selon la gravité des infractions, alors même que le législateur belge a estimé devoir préciser cela dans la loi[18].

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

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

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

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

---

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

16 *Ibidem*, §79-80.

17 *Ibidem*, §82 AG

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

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

Luxembourg, le 13 avril 2023

Georges OSWALD
Procureur d'Etat à Luxembourg

Ernest NILLES
Procureur d'Etat à Diekirch

Impression: CTIE – Division Imprimés et Fournitures de bureau