N° 8148[6]

CHAMBRE DES DEPUTES

PROJET DE LOI

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

1° du Code de procédure pénale ;

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

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

* * *

AVIS DE LA COMMISSION NATIONALE POUR LA PROTECTION DES DONNEES

(16.5.2024)

1. Conformément à l'article 57.1.c) 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) (ci-après le « RGPD »), auquel se réfère l'article 7 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, la Commission nationale pour la protection des données (ci-après la « Commission nationale » ou la « CNPD ») « *conseille, conformément au droit de l'État membre, le parlement national, le gouvernement et d'autres institutions et organismes au sujet des mesures législatives et administratives relatives à la protection des droits et libertés des personnes physiques à l'égard du traitement* ».

Par ailleurs, l'article 36.4 du RGPD dispose que « *[l]es États membres consultent l'autorité de contrôle dans le cadre de l'élaboration d'une proposition de mesure législative devant être adoptée par un parlement national, ou d'une mesure réglementaire fondée sur une telle mesure législative, qui se rapporte au traitement* ».

2. Par courrier en date du 2 février 2023, Madame la Ministre de la Justice a invité la Commission nationale à se prononcer sur le projet de loi n°8148 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 (ci-après le « projet de loi »).

3. Selon l'exposé des motifs, le projet de loi a pour objet de « *répondre aux exigences de la jurisprudence européenne en permettant une conciliation entre les deux exigences que sont sécurité et liberté* »[1]. La Cour de justice de l'Union européenne (ci-après la « CJUE » ou la « Cour ») a depuis le premier arrêt en la matière en 2014[2] détaillé de plus en plus sa position quant à la possibilité pour les opérateurs de télécommunications ou les fournisseurs de services de communications électroniques

1 Doc. parl. de dépôt, p. 17.

2 Arrêt du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238.

(ci-après les « opérateurs et fournisseurs ») de conserver des données de trafic et de localisation et pour les autorités nationales compétentes d'accéder aux données ainsi conservées.

4. La Cour soulève qu'une telle conservation par les opérateurs et fournisseurs va à l'encontre du principe de confidentialité consacré par la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (ci-après la « directive vie privée et communications électroniques »). Ainsi, les données de trafic et de localisation doivent en principe être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication.

5. Ce principe d'effacement subit pourtant des dérogations, notamment en ce qui concerne la conservation de données requises pour établir les factures et les paiements pour interconnexion, voire encore la possibilité avec le consentement de la personne concernée de traiter ces données à des fins commerciales ou de fourniture de services à valeur ajoutée. Une autre dérogation découle de l'article 15 de cette directive qui accorde la possibilité aux États membres de limiter la portée des droits et des obligations dans certains cas.

6. La jurisprudence en matière de rétention des données porte ainsi essentiellement sur l'interprétation de la Cour sur les dérogations possibles en application de l'article 15 de la directive vie privée et communications électroniques. Dans les arrêts[3] qui ont suivi le premier arrêt « Digital Rights Ireland » du 8 avril 2014, la Cour décline de plus en plus cette interprétation et fournit des indications quant aux modalités qui doivent accompagner ces dérogations admissibles au principe de confidentialité.

7. La CJUE détermine ainsi que l'article 15 de la directive vie privée et communications électroniques, lu à la lumière de la Charte des droits fondamentaux de l'Union européenne, ne s'oppose pas à des mesures législatives nationales prévoyant tant la conservation de données de trafic et de localisation que l'accès à ces données pour autant qu'elles soient limitées en ce qui concerne les objectifs recherchés ainsi que délimitées en ce qui concerne les personnes visées, les moyens de communications ciblés, les catégories de données conservées et la durée de conservation retenue et qu'elles « *assurent, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus* »[4].

8. Au fil des dernières années, la CJUE a pu analyser, dans les arrêts relatifs à la rétention des données, différentes mesures législatives de conservation et d'accès ayant tenté de répondre aux exigences soulevées dans sa jurisprudence. Par conséquent, elle a pu préciser de plus en plus ce que des mesures législatives de conservation et d'accès doivent respecter afin d'être conformes au cadre légal en matière de protection des données à caractère personnel. L'exposé des motifs décrit extensivement la majorité des exigences soulevées par la CJUE.

9. De manière générale, la CNPD souhaite néanmoins rappeler que pour assurer la conformité au principe de proportionnalité, la CJUE a exprimé à plusieurs reprises que la conservation doit être limitée au strict nécessaire pour atteindre les objectifs. Dans ses arrêts, la CJUE procède de manière systématique pour analyser la proportionnalité des mesures.

---

3 Arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C :2016:970 ;
arrêt du 2 octobre 2018, Ministerio Fiscal C-207/16, EU:C:2018:788 ;
arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791 ;
arrêt du 6 octobre 2020, Privacy International, C-623/17, EU:C:2020:790 ;
arrêt du 2 mars 2021, Prokuratuur, C-746/18, EU:C:2021:152 ;
arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258 ;
arrêt du 20 septembre 2022, SpaceNet et Telekom Deutschland C-793/19 et c-794/19, EU:C:2022:702 ;
arrêt du 17 novembre 2022, Spetsializirana prokuratura C-350/21, EU:C:2022:896 ;
arrêt du 30 avril 2024, Procura della Repubblica presso il Tribunale di Bolzano, C-178/22, EU:C:2024:371 ;
arrêt du 30 avril 2024, La Quadrature du Net e.a. (Données personnelles et lutte contre la contrefaçon), C-470/21, EU:C:2024:370.

4 Voir arrêt du 20 septembre 2022, SpaceNet et Telekom Deutschland C-793/19 et c-794/19, EU:C:2022:702, point 132.

10. Ainsi, en premier lieu, elle détermine les finalités recherchées par les mesures législatives de conservation ou d'accès. Cette première étape est essentielle, non seulement parce que les finalités sont listées de manière exhaustive[5] dans l'article 15 de la directive vie privée et communications électroniques, mais également parce que l'importance de l'objectif recherché a un impact sur l'ingérence tolérée sur la vie privée des personnes concernées. Force est de constater à la lecture des arrêts de la CJUE en matière de rétention de données que plus les objectifs sont importants, plus l'ingérence des mesures de conservation et d'accès dans la vie privée des personnes concernées est tolérée.

11. Il en résulte que l'étendue des mesures législatives de conservation et d'accès dépend largement de l'objectif recherché. Ainsi, une conservation généralisée et indifférenciée des données relatives au trafic peut être tolérée, sous réserve de respecter certaines conditions, pour les objectifs de préservation de la sécurité nationale. Or, pour la lutte contre la criminalité grave, il est nécessaire de limiter l'étendue des mesures de conservation ou d'accès sur base de critères objectifs et non discriminatoires. Cette limitation peut se rapporter aux personnes concernées, aux catégories de données, aux zones géographiques, voire encore aux moyens de communications utilisés. En matière de criminalité simple[6], la CJUE est encore plus exigeante.

12. En deuxième lieu, la CJUE apprécie tant la durée des mesures de conservation et d'accès que la durée de conservation des données proprement dites. En ce qui concerne la durée de conservation des données, la CJUE retient qu'elle doit être limitée au strict nécessaire pour atteindre l'objectif recherché[7] et être choisie sur base de critères objectifs[8]. En ce qui concerne la durée d'application des mesures, la CJUE ne s'est jusqu'à présent prononcée que sur les mesures concernant l'accès aux données conservées. Dans ce contexte, elle explique que l'accès « *présente en tout état de cause un caractère grave indépendamment de la durée de la période pour laquelle l'accès auxdites données est sollicité et de la quantité ou de la nature des données disponibles pour une telle période, lorsque […] cet ensemble de données est susceptible de permettre de tirer des conclusions précises sur la vie privée de la ou des personnes concernées* »[9], et qu'il doit se limiter au strict nécessaire[10].

13. Enfin, la CJUE exige que les mesures législatives permettent « *d'assurer une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès et toute utilisation illicite de ces données* »[11]. Ces garanties s'imposent non seulement pour les mesures législatives de conservation[12], mais également pour les mesures législatives d'accès[13] aux données stockées.

14. Selon l'exposé des motifs, le projet de loi sous avis a pour objet « *d'encadrer la conservation et l'usage des données de trafic et de localisation sans priver ces données de leur valeur utile, notamment en fixant des conditions strictes d'accès et de durée de conservation* »[14].

15. Pour ce faire, le projet de loi entend supprimer de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques relatif au projet de loi n°8148 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 (dénommée ci-après la « loi Télécom ») l'obligation de conservation généralisée et indifférenciée de toutes les données de trafic et de

---

5 Voir arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 112.

6 Voir arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, points 110 et 111.

7 Voir arrêt du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 63.

8 Voir arrêt du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 64, et arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 108.

9 Voir arrêt du 2 mars 2021, Prokuratuur, C-746/18, EU:C:2021:152, point 39.

10 Voir arrêt du 2 mars 2021, Prokuratuur, C-746/18, EU:C:2021:152, point 38.

11 Voir arrêt du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 66.

12 Voir arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 122, qui impose aux fournisseurs de service de communications électroniques une conservation des données sur le territoire de l'Union européenne.

13 Voir arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 121, qui impose aux autorités d'informer les personnes concernées de l'accès, dans la mesure où cette information ne risque pas de compromettre les enquêtes menées.

14 Doc. parl. de dépôt, p.17.

localisation pour tous les objectifs énumérés à l'article 15 de la directive vie privée et communications électroniques. En tant que substitut, il entend introduire plusieurs mesures législatives de conservation des données et d'accès à ces données qui sont censées répondre aux exigences de la CJUE.

16. En droit interne, la Constitution garantit que les libertés publiques des citoyens sont respectées. Dans le contexte du présent projet de loi, ces sont notamment les libertés publiques consacrées aux articles 20 (vie privée), 30 (inviolabilité des communications) et 31 (protection des données) de la Constitution qui sont en jeu dans le cadre du présent projet de loi. De plus, l'article 37 de la Constitution dispose que « *[t]oute limitation de l'exercice des libertés publiques doit être prévue par la loi […]*».

17. Il importe encore de mentionner l'article 8.2 de la Convention européenne des droits de l'homme concernant le droit au respect de la vie privée, ainsi que la jurisprudence s'y rapportant. Cette disposition prévoit qu'« *[i]l ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui* ». Pour déterminer la conformité à l'article 8.2, la Cour européenne des droits de l'homme (ci-après la « CEDH ») recherche si l'ingérence est prévue par la loi, poursuit un/des but(s) légitime(s) et si elle est proportionnée à ce(s) but(s).

18. La CNPD ayant déjà abordé cet aspect, en particulier celui de la proportionnalité ainsi que de la prévisibilité de la loi dans d'autres avis, elle se limite à renvoyer à ces observations[15].

19. La CEDH admet néanmoins une atténuation pour le critère de prévisibilité de la loi en matière de surveillance secrète : « *La Cour a jugé à plusieurs reprises que, en matière d'interception de communications, la «* prévisibilité *» ne pouvait se comprendre de la même façon que dans beaucoup d'autres domaines. Dans le contexte particulier des mesures de surveillance secrète, telle l'interception de communications, la prévisibilité ne saurait signifier qu'un individu doit se trouver à même de prévoir quand les autorités sont susceptibles d'intercepter ses communications de manière qu'il puisse adapter sa conduite en conséquence* »[16].

20. Cette atténuation est applicable en matière de rétention des données, étant donné que la CEDH qualifie la conservation de données de trafic et de localisation comme une mesure de surveillance secrète dont le degré d'ingérence dans la vie privée des personnes concernées équivaut à celui de l'interception du contenu de la communication[17]. La conservation et l'accès aux données de trafic et de localisation doivent dès lors bénéficier des mêmes sauvegardes que les mesures de surveillance secrète[18]. *Ainsi, « […] le risque d'arbitraire apparaît avec netteté là où un pouvoir de l'exécutif s'exerce en secret. L'existence de règles claires et détaillées en matière d'interception de conversations téléphoniques apparaît donc indispensable, d'autant que les procédés techniques utilisables ne cessent de se perfectionner. La loi doit être rédigée avec suffisamment de clarté pour indiquer à tous de manière adéquate en quelles circonstances et sous quelles conditions elle habilite la puissance publique à prendre pareilles mesures secrète* »[19].

21. La CEDH ajoute encore que la loi doit, de manière suffisamment claire, définir l'étendue et les modalités de l'exercice du pouvoir d'appréciation de l'autorité qui ordonne la mesure de surveillance pour éviter l'arbitraire. Elle « *énonce les garanties minimales suivantes contre les abus de pouvoir que la loi doit renfermer : la nature des infractions susceptibles de donner lieu à un mandat d'interception, la définition des catégories de personnes susceptibles d'être mises sur écoute, la fixation d'une limite à la durée d'exécution de la mesure, la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies, les précautions à prendre pour la communication des données à d'autres*

---

15 Voir délibération n°3/AV3/2021 du 10 février 2021, Point 11.2.

16 Voir arrêt de la CEDH du 4 décembre 2015, Roman Zakharov c. Russie, point 229.

17 Voir arrêt de la CEDH du 11 janvier 2022, Ekimdzhiev et autres c. Bulgarie, point 394.

18 *Ibid*, point 295.

19 Voir arrêt de la CEDH du 4 décembre 2015, Roman Zakharov c. Russie, point 229.

parties, et les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements »[20].

22. Concernant la condition que la mesure doit être nécessaire dans une société démocratique, la CEDH précise que des garanties adéquates et effectives doivent exister afin d'éviter l'arbitraire et les abus. Elle estime que l'existence d'un contrôle de la nécessité de la mesure est une telle garantie et que l'appréciation doit se faire en prenant en compte toutes les circonstances de l'affaire en question. La CEDH explique encore que le contrôle peut se faire à trois moments : au moment où la mesure est ordonnée, pendant l'exécution et lorsque la mesure est terminée.[21]

23. Afin d'apprécier si les différentes mesures législatives prévues par le projet de loi respectent les exigences de la CJUE et de la CEDH, il est nécessaire de différencier entre les mesures législatives de conservation de données (1) et les mesures législatives d'accès à ces données (II). Enfin, il convient encore d'examiner les autres modifications (III) que le projet de loi entend apporter.

*

I. LES MESURES LEGISLATIVES DE CONSERVATION DE DONNEES

24. Le projet de loi opère un changement de paradigme en ce qu'il introduit le principe de l'interdiction d'une conservation généralisée et indifférenciée des données de trafic et de localisation. Il ressort du commentaire des articles que « *[c]ontrairement au libellé introduit par la Loi Telecom [...] 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* ».

25. Il est effectivement de jurisprudence constante que le principe de confidentialité est d'interprétation stricte[22]. Ainsi, la Cour a pu confirmer à plusieurs reprises qu'une dérogation à ce principe sur base de l'article 15 de la directive vie privée et communications électroniques ne peut pas, en ce qui concerne notamment la conservation de ces données, devenir la règle mais doit toujours rester l'exception et doit respecter le principe de nécessité.

26. La CJUE fournit dans ses arrêts les exigences à prendre en compte afin de garantir une conservation limitée au strict nécessaire. Ces délimitations peuvent jouer au niveau des finalités et/ou de l'étendue de la mesure. Etant donné que l'exposé des motifs reprend fidèlement les exigences que la CJUE a rattaché à chacune de ces catégories, le présent avis se limite à renvoyer à ces explications[23].

27. La CJUE répartit les mesures législatives de conservation des données en trois grandes catégories, à savoir la conservation ciblée, la conservation généralisée et indifférencié et la conservation rapide.

28. A la lecture du projet de loi, il devient clair que les auteurs introduisent ces trois catégories de mesures, dont certaines doivent être ordonnées (A) par le juge d'instruction, le procureur ou le service de renseignement (ci-après le « SRE ») tandis que d'autres résultent d'une obligation légale de conservation (B).

29. De plus, la CJUE exige que la conservation des données de trafic et de localisation soit entourée de garanties suffisantes et appropriées par les opérateurs et fournisseurs. Comme chaque mesure de conservation doit répondre à cette exigence, il convient de regrouper les observations y relatives dans une section dédiée (C).

---

20 *Ibid*., points 230 et 231.

21 *Ibid*., points 232 et 234.

22 Voir arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 89.

23 Doc. parl. de dépôt, p. 11 à 15.

A. Les mesures de conservation devant être ordonnées

1. *La mesure de conservation du nouvel article 24-3 du Code de procédure pénale*

30. L'article 1er, point 1° du projet de loi introduit un nouvel article 24-3 dans le Code de procédure pénale (ci-après le « CPP ») ayant comme objectif de mettre à la disposition du procureur d'État une mesure de conservation des données de trafic et de localisation. Ainsi, le procureur d'État peut ordonner dans le cadre 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 la conservation des données relatives au trafic et à la localisation qu'il juge nécessaires.

31. La CNPD partage la confusion exprimée par les Parquets du Tribunal d'Arrondissement de Luxembourg et de Diekirch dans leur avis commun en ce qu'il n'est pas clair si la mesure de conservation vaut pour les données déjà générées ou traitées par les opérateurs et fournisseurs ou si elle vaut pour les données qui seront encore générées ou traitées par les opérateurs et fournisseurs à partir de la date de l'ordonnance[24]. Le commentaire des articles contribue davantage à la confusion comme les auteurs du projet de loi parlent tant de la mesure comme conservation ciblée que « *d'une sorte de « quick freeze »* [conservation rapide] *pour le futur* »[25]. Ainsi, il n'est pas tout à fait clair si la nouvelle mesure est une mesure de conservation ciblée ou une mesure de conservation rapide.

32. D'après la compréhension de la CNPD, la conservation ciblée ainsi que la conservation rapide telles que décrites par la CJUE sont deux mesures législatives distinctes, avec notamment des exigences distinctes. En effet, pour la conservation rapide, la CJUE exige notamment que « *[d]ans la mesure où la finalité d'une telle conservation rapide ne correspond plus à celles pour lesquelles les données ont été collectées et conservées initialement et où tout traitement de données doit, en vertu de l'article 8, paragraphe 2, de la Charte, répondre à des fins déterminées, les États membres doivent préciser, dans leur législation, la finalité pour laquelle la conservation rapide des données peut avoir lieu* »[26]. Cette exigence s'explique par le fait que le traitement initial des opérateurs et fournisseurs avait une finalité commerciale. Or, après l'ordonnance de conservation rapide, une nouvelle finalité s'ajoute à cette finalité initiale. Cette nouvelle finalité de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, devrait dès lors être ancrée dans la loi.

33. Enfin, d'après la description fournie par la CJUE, la conservation rapide devrait servir à conserver les données dont il existe un risque de perte ou de modification. Il s'agit donc d'une mesure qui s'applique à des données existantes et déjà détenues par les opérateurs et fournisseurs, plutôt qu'à des données qui seront générées ou traitées dans le futur[27]. Ainsi, la CNPD se demande si le nouvel article 24-3 du CPP ne se limite pas à introduire une conservation ciblée plutôt qu'une conservation rapide.

34. Tel que revendiqué par les Parquets du Tribunal d'Arrondissement de Luxembourg et de Diekirch dans leur avis commun, des clarifications quant à la mesure législative visée par l'article 24-3 du CPP devraient être apportées, notamment pour préciser si elle se rapporte aux données déjà générées ou traitées, et/ou aux données qui seront générées ou traitées dans le futur[28]. Si effectivement les auteurs du projet de loi visent les deux cas de figure, c'est-à-dire les données futures et les données existantes, se pose alors la question s'il ne serait pas plus clair de prévoir deux dispositions séparées.

---

24 Avis commun des Parquets du Tribunal d'Arrondissement de Luxembourg et de Diekirch du 13 avril 2023, doc. parl. n°8148/03, p.3.

25 Doc. parl. de dépôt, p.18.

26 Arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 164 et arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 87.

27 Arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, points 162 et 163.

28 Avis commun des Parquets du Tribunal d'Arrondissement de Luxembourg et de Diekirch du 13 avril 2023, doc. parl. n°8148/03, p.3.

35. Par ailleurs il serait intéressant de savoir pourquoi les auteurs du projet de loi n'ont pas rajouté la mesure de conservation ciblée à l'article 24-1 du CPP régissant la « mini-instruction ». D'autant plus qu'un contrôle juridictionnel effectif serait alors garanti et qu'un lien avec l'article 67-1 du CPP traitant de l'accès aux données ainsi conservées serait établi. D'après la compréhension de la CNPD, il ressort des travaux parlementaires de l'article 67-1 du CPP que le juge d'instruction peut ordonner l'accès aux données conservées par les opérateurs et fournisseurs ainsi que la conservation de données futures. Le recours à la mini-instruction serait dès lors envisageable, à condition que l'article 67-1 du CPP respectent les exigences de le CJUE.

36. Dans le même ordre d'idées, la CNPD se demande pourquoi les auteurs du projet de loi, si la mesure sous avis devrait être une mesure de conservation rapide, ne l'ont pas ajoutée au Chapitre X du CPP prévoyant la conservation rapide des données informatiques à disposition du juge d'instruction et du procureur d'État.

37. Dans tous les cas, les mesures législatives doivent répondre aux exigences de la CJUE. Partant, dans l'hypothèse où le nouvel article 24-3 du CPP régit une mesure de conservation ciblée des données de trafic et de localisation, elle ne peut être prise qu'« *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* »[29]. Par ailleurs, elle doit être « *délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable* »[30]. La Cour précise encore qu'une telle mesure doit assurer, « *par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus* »[31].

38. Concernant les finalités pour lesquelles on peut recourir à une mesure de conservation ciblée, la jurisprudence de l'Union européenne admet que ce n'est possible qu'« *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* »[32].

39. Il y a lieu de constater que le nouvel article 24-3 du CPP retient un seuil comme critère de délimitation, à savoir les infractions pénales qui emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement. La CNPD partage l'appréciation du Conseil d'État que « *les infractions sanctionnées par une peine d'emprisonnement égale ou supérieure à un an ne relevant de surcroit pas toutes de la criminalité grave* »[33]. Ainsi, il convient de se demander si le seuil fixé est suffisamment élevé. La CNPD réitère dès lors sa préférence exprimée dans plusieurs avis[34] pour une liste limitative d'infractions qualifiées de graves. Une liste limitative permettrait de réserver les mesures législatives aux enquêtes et aux actes de poursuite relatifs à des infractions qui se situent clairement dans le contexte de la criminalité grave.

40. Les auteurs du projet de loi expliquent qu'il s'agit d'un choix politique national comme la notion ne connaît pas de définition harmonisée au niveau de l'Union européenne[35]. Dans un arrêt récent, la CJUE confirme cette approche[36] toute en rappelant que « *la définition des* « infractions graves »*, opérée par les États membres, doit respecter les exigences qui découlent de cet article 15, paragraphe 1, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte* »[37].

---

29 Arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 168.

30 *Ibid.*

31 *Ibid.*

32 *Ibid.*

33 Voir avis du Conseil d'État du 23 janvier 2024, doc. parl. 8148/05, p.4.

34 Voir par exemple avis n°85/2010 du 24 avril 2010 et avis n°214/2014 du 13 mai 2014.

35 Doc. parl. de dépôt, p.20 et suivants.

36 Arrêt du 30 avril 2024, Procura della Repubblica presso il Tribunale di Bolzano, C-178/22, EU:C:2024:371, points 44 à 47.

37 *Ibid*., point 47.

41. A cet égard, la Cour souligne que « *les États membres ne sauraient dénaturer la notion d'« infraction grave » et, par extension, celle de* « criminalité grave »*, en y incluant, aux fins de l'application de cet article 15, paragraphe 1, des infractions qui ne sont manifestement pas graves, au regard des conditions sociétales prévalant dans l'État membre concerné, alors même que le législateur de cet État membre a prévu de les punir d'une peine maximale de réclusion de trois ans* »[38].

42. Même si la Cour ne propose pas de définition pour les notions d'« infraction grave » ou de « criminalité grave », elle donne néanmoins des considérations à prendre en compte par les États membres. Ainsi, la Cour ne rejette pas le concept que la gravité de l'infraction est déterminée par un seui1[39]. En effet, la Cour estime qu'un seuil fixé par la loi est un critère objectif permettant de déterminer le degré de gravité d'une infraction.

43. Or, la Cour soulève également que le seuil choisi par les États membres « *ne doit pas être à ce point large que l'accès à ces données devienne la règle plutôt que l'exception* »[40]. Elle ajoute que la notion de « criminalité grave » ou d'« infraction grave », ne doit pas « *couvrir la grande majorité des infractions pénales, ce qui serait le cas si le seuil au-delà duquel la peine de réclusion maximale dont est punie une infraction justifie que celle-ci soit qualifiée d'infraction grave était fixé à un niveau excessivement bas* »[41].

44. Toujours en ce qui concerne la détermination des infractions graves par un seuil, la Cour soulève encore que « *par référence non pas à une peine minimale applicable mais à une peine maximale applicable, il n'est pas exclu qu'un accès à des données, constitutif d'une ingérence grave dans les droits fondamentaux, puisse être demandé à des fins de poursuites d'infractions ne relevant pas, en réalité, de la criminalité grave* »[42]. Elle estime néanmoins que ceci n'est « *pas nécessairement contraire au principe de proportionnalité* »[43].

45. Afin d'apprécier si la proportionnalité est garantie lorsqu'un seuil fait référence à une peine maximale, la CJUE estime qu'il faut veiller à deux choses. Premièrement, il convient de vérifier si la disposition législative vise de « *manière générale l'accès aux données conservées [...] sans préciser la nature de ces données* »[44]. La Cour estime que s'il n'est pas précisé dans la disposition quelles données sont accédées et que ceci est à la libre appréciation des autorités demandant l'accès, il est possible que la mesure en question ne se limite pas aux infractions graves. Effectivement, si l'autorité se limite à demander l'accès à des données ne permettant pas des conclusions précises sur la vie privée des personnes concernées, cet accès ne peut pas être qualifié de grave et est possible pour les infractions dites simples[45].

46. Il en résulte que, deuxièmement, une juridiction ou une entité administrative indépendante intervenant dans le cadre du contrôle préalable doit apprécier le degré de gravité de l'ingérence dans la vie privée par rapport à la gravité de l'infraction. Lorsqu'il découle de ce contrôle préalable que le degré d'ingérence dans la vie privée n'est pas proportionnée au degré de l'infraction, la juridiction ou l'autorité administrative « *doit être habilitée à refuser ou à restreindre cet accès* »[46] car cette entité « *doit être en mesure d'assurer un juste équilibre entre, d'une part, les intérêts légitimes liés aux besoins de l'enquête dans le cadre de la lutte contre la criminalité et, d'autre part, les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel des personnes dont les données sont concernées par l'accès* »[47].

---

38 *Ibid*., point 50.
39 *Ibid*., point 54.
40 *Ibid*., point 55.
41 *Ibid*.
42 *Ibid*., point 57.
43 *Ibid*., point 58.
44 *Ibid*., point 59.
45 *Ibid.*
46 *Ibid*., point 60.
47 *Ibid*., point 61.

47. Dans la mesure où le projet de loi sous avis entend délimiter la criminalité grave de la criminalité simple par référence à un seuil de peine maximale, les critères énoncés par la CJUE doivent être pris en considération. Or, comme cette jurisprudence de la CJUE est postérieure au dépôt du projet de loi, il serait judicieux de revoir les mesures législatives prévues et de les conformer, le cas échéant, aux exigences de la CJUE. En ce qui concerne le seuil fixé, il peut, tel que déjà susmentionné, être remis en doute s'il est suffisamment élevé. Ensuite, en ce qui concerne le principe de proportionnalité, il convient de vérifier pour chaque mesure individuellement si les critères soulevés par la CJUE sont prévus.

48. La CNPD souhaite encore attirer l'attention du législateur au règlement (UE) 2018/1240 du Parlement européen et du Conseil du 12 septembre 2018 portant création d'un système européen d'information et d'autorisation concernant les voyages (ETIAS) et modifiant les règlements (UE) 1077/2011, (UE) 515/2014, (UE) 2016/399, (UE) 2016/1624 et (UE) 2017/2226 qui dans son article 3.1. point 16 définit l'infraction pénale grave comme « *une infraction qui correspond ou est équivalente à l'une des infractions visées à l'article 2, paragraphe 2, de la décision-cadre 2002/584/JAI, si elle est passible, en droit national, d'une peine ou d'une mesure de sûreté privative de liberté d'une durée maximale d'au moins trois ans* ». La CNPD se demande dès lors si cette définition ne pourrait pas servir de source d'inspiration pour le projet de loi sous avis.

49. Ensuite, en ce qui concerne l'étendue de la mesure législative prévoyant la conservation ciblée, la CJUE exige qu'elle soit prévue dans la loi nationale et limitée par des critères objectifs et non discriminatoires[48]. Or, il y a lieu de constater que la rédaction actuelle de l'article 24-3.1 alinéa 3 du CPP se limite à prévoir que la décision écrite et motivée du procureur d'État contient « *b) [l]'indication précise d'un ou de plusieurs des éléments suivants : la ou les personnes, les moyens de communications ou les lieux qui font l'objet de la conservation* ». La disposition ne contient pas de critères permettant de délimiter exactement les personnes, lieux ou moyens de communication à viser par la conservation.

50. Dans la mesure où le futur article 24-3 du CPP prévoit une conservation ciblée, la CNPD se demande dès lors s'il ne devrait pas contenir des critères permettant de délimiter les zones géographiques ou les personnes pouvant être visées par la mesure tel que préconisé par la CJUE ou encore la CEDH. Les auteurs du projet de loi auraient pu s'inspirer des éléments fournis par la Cour dans ses arrêts successifs[49] ainsi que des critères prévus au nouvel article *5bis* de la loi Télécom.

51. La Cour clarifie par ailleurs qu'à part une délimitation des personnes ou zones visées par la mesure, « *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 et d'établir un lien, au moins indirect, entre les actes de criminalité grave et les personnes dont les données sont conservées. Cela étant, l'article 15, paragraphe 1, de la directive 2002/58 visant des mesures législatives des États membres, c'est à ces derniers et non à la Cour qu'il incombe d'identifier de tels critères, étant entendu qu'il ne saurait être question de réinstaurer, par ce biais, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation* »[50]. Il existe donc éventuellement d'autres critères non énumérés par la CJUE qui pourrait servir pour délimiter l'étendue de la mesure.

52. Concernant les catégories de données qui peuvent potentiellement être conservées, le futur article 24-3.1 alinéa 2 du CPP prévoit qu'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 poursuit d'infractions visées ci-dessus* ». La CNPD se rallie aux observations du Conseil d'État à ce sujet[51]. Elle ajoute que la jurisprudence de la CJUE énonce que pour la conservation ciblée, il appartient à la loi de contenir les critères objectifs et non discriminatoires qui permettent de déterminer quelles catégories de données peuvent être conservées. Il ne suffit dès lors pas de fixer les catégories de données

---

48 Arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 76

49 Voir en ce sens par exemple, l'arrêt du 20 septembre 2022, SpaceNet et Telekom Deutschland C-793/19 et c-794/19, EU:C:2022:702, points 104 à 113.

50 Arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 83.

51 Voir avis du Conseil d'État du 23 janvier 2024, doc. parl. 8148/05, p.4 et 5.

qui peuvent être collectées, mais il faut bien prévoir des critères sur base desquels on limite au strict nécessaire les données pouvant être collectées.

53. Par ailleurs, il ne ressort pas clairement de la disposition que le règlement grand-ducal visé correspond à celui pris initialement sur base de l'article 5 de le loi Télécom, à savoir 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. A l'instar des Parquets du Tribunal d'Arrondissement de Luxembourg et de Diekirch dans leur avis commun[52], la CNPD est d'avis qu'il doit être clair à la lecture de l'article 24-3 du CPP quel règlement grand-ducal est visé.

54. Concernant le règlement grand-ducal proprement dit, la CNPD est d'avis que sa rédaction devrait être adapté au nouveau régime. Le libellé de l'article 3 dudit règlement reflète dès lors toujours la logique d'une obligation légale de conservation généralisée et indifférenciée des données listées. La CNPD estime pourtant que le règlement grand-ducal devrait contenir une liste exhaustive de données qui constituent des données de trafic ou de localisation parmi lesquelles le procureur d'État doit choisir sur base de critères objectifs et non discriminatoires prévus par la loi celles qui sont nécessaires à la réalisation de son objectif.

55. Dans le même ordre d'idée, il convient de se demander pourquoi les auteurs ont choisi d'inclure dans le paragraphe 1er alinéa 2, les appels infructueux. En effet, déjà en 2010 lorsque ce concept a été introduit dans la loi Télécom, le Conseil d'État avait constaté que cette précision était superflue car « *peu importe si un appel est fructueux ou infructueux, il constitue une donnée du trafic* »[53].

56. Par ailleurs, tel qu'expliqué par les Parquets du Tribunal d'Arrondissement de Luxembourg et de Diekirch dans leur avis commun[54], il reste à clarifier si le contrôle juridictionnel existant pour l'ordonnance du procureur d'État respecte les exigences de la CJUE[55] ou encore de la CEDH[56] en la matière.

57. Ensuite, en ce qui concerne la durée de conservation retenue, l'article 24-3 du CPP prévoit une durée de 6 mois, prolongeable si nécessaire. Or, il y a lieu de constater que le projet de loi ne prévoit pas de durée d'application de la mesure. Il est dès lors impossible de déterminer le moment à partir duquel il faut compter les 6 mois de durée de conservation. La CNPD se demande par conséquent si la disposition ne devrait pas être complétée par une durée d'application de la mesure, prévoyant ainsi la période sur laquelle les opérateurs et fournisseurs doivent procéder à la conservation. Une fois que la durée d'application de la mesure prend fin, la durée de conservation des données commence à courir.

58. En ce qui concerne la durée de conservation proprement dite, à savoir 6 mois prolongeable, la CNPD regrette que les auteurs du projet de loi n'aient pas fourni d'explication quant au choix retenu. Elle se voit dès lors dans l'impossibilité d'apprécier la proportionnalité de la durée choisie. La CNPD se rallie par ailleurs au Conseil d'État. La Haute Corporation soulève en effet que la disposition « *est en outre source d'insécurité juridique étant donné qu'une prolongation d'un délai, contrairement à sa reconduction, ne donne pas de limite précise à la mesure, entraînant de ce fait une imprécision quant à sa durée* »[57].

59. Concernant la destruction des données à la fin de la durée de conservation prévue au paragraphe 2 du nouvel article 24-3 du CPP, il convient de soulever que la disposition prête à confusion.

---

52 Avis commun des Parquets du Tribunal d'Arrondissement de Luxembourg et de Diekirch du 13 avril 2023, doc. parl. n°8148/03, p.2.

53 Avis du Conseil d'État sur le projet de loi n°6113 portant modification des articles 5 et 9 de la loi modifiée du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications électroniques et de l'article 67-1 du Code d'instruction criminelle, doc. parl. 6113/06, p.3.

54 Avis commun des Parquets du Tribunal d'Arrondissement de Luxembourg et de Diekirch du 13 avril 2023, doc. parl. n°8148/03, p.3

55 Arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 85, et jurisprudence citée

56 Voir arrêt de la CEDH du 11 janvier 2022, Ekimdzhiev et autres c. Bulgarie, point 301.

57 Voir avis du Conseil d'État du 23 janvier 2024, doc. parl. 8148/05, p.4.

En effet, il semble que cette disposition reflète une obligation pour les opérateurs et fournisseurs en ce qu'ils doivent détruire les données une fois la durée de conservation venue à échéance. Or, comme l'article 24-3 du CPP encadre une mesure d'enquête préalable à disposition du procureur d'État, il ne ressort pas naturellement du texte que l'obligation de destruction s'adresse aux opérateurs et aux fournisseurs.

60. Ensuite, il convient de s'interroger sur l'exception au principe de destruction introduite par la deuxième partie de la phrase unique constituant le paragraphe 2 de l'article 24-3 du CPP. Ainsi, les données conservées au titre de l'article 24-3 du CPP auxquelles les autorités compétentes ont accédé ou qu'elles ont préservées ne sont pas détruites. Se pose alors la question de la durée de conservation ultime pour les données qui seront malgré tout conservées. De plus, la CNPD s'interroge sur la raison de cette conservation supplémentaire. Si les autorités compétentes ont préservé les données conservées utiles pour l'enquête, quelle est la raison pour laquelle les opérateurs et fournisseurs doivent les conserver au-delà de la durée initiale ? Il en va de même pour les données qu'ils ont accédées mais qu'ils n'ont pas jugé utiles pour préserver. Pourquoi les opérateurs et fournisseurs doivent les conserver ?

61. De plus, l'article 24-3 du CPP dans sa rédaction actuelle ne contient pas d'indication ou de référence vers la ou les dispositions encadrant l'accès aux données conservées. La CNPD se rallie à l'observation des Parquets du Tribunal d'Arrondissement de Luxembourg et de Diekirch dans leur avis commun[58] qu'une référence à l'article 67-1 du CPP qui selon les auteurs du projet de loi constitue le fondement de l'accès devrait être introduite.

62. De manière similaire, la CNPD s'interroge sur le renouvellement prévu par l'article 24-3.1 alinéa 3 point c) du CPP. Ne s'agit-il pas plutôt d'un renouvellement de la durée d'application de la mesure que de la durée de conservation des données stockées par les opérateurs et fournisseur? Une précision à cet égard serait souhaitable.

63. De plus, à l'instar du Parquet général[59] et du Conseil d'État[60], la CNPD se demande quelles conditions de forme et de fond devraient être remplies afin d'obtenir une prolongation de ce délai.

64. Enfin, l'article 24-3.1 alinéa 4 du CPP prévoit qu'en cas d'urgence, le procureur d'État peut ordonner verbalement la mesure de conservation et devra par la suite la confirmer dans les meilleurs délais par écrit dans la forme prévue à l'alinéa 3. Il convient de s'interroger s'il ne serait pas utile de prévoir un délai maximal précis pour le procureur d'État de confirmer sa décision orale.

2. *La mesure de conservation de l'article 67-1 du Code de procédure pénale*

65. Selon l'exposé des motifs, « *[l]'obligation de conservation des données de trafic et de localisation relatives aux communications électroniques a été introduite dans la législation luxembourgeoise par la loi du 30 mai 2005 concernant la protection de la vie privée dans le secteur des communications* ». Toujours selon l'exposé des motifs, « *[l]es opérateurs nationaux sont donc tenus à conserver les données de trafic et de localisation au sens des articles 5 et 9 de la Loi Telecom et l'accès à ces données est garanti au juge d'instruction moyennant l'article 67-1 du Code de procédure pénale […]* ».

66. L'article 67-1 du CPP semble donc régir uniquement l'accès aux données conservées et non pas la conservation des données proprement dite. Or, les travaux parlementaires de la loi ayant introduit l'article 67-1 dans le Code de procédure pénale expliquent que la mesure de repérage « *peut viser aussi bien les communications passées que les communications futures* »[61]. Le Conseil d'État avait soulevé dans son avis à l'époque que le repérage « *ne devrait viser que l'obtention de données d'appel déjà*

---

58 Avis commun des Parquets du Tribunal d'Arrondissement de Luxembourg et de Diekirch du 13 avril 2023, doc. parl. n°8148/03, p.2.

59 Avis du Parquet général du 13 mars 2023, doc. parl. n°8148/02, p.6.

60 Voir avis du Conseil d'État du 23 janvier 2024, doc. parl. 8148/05, p.5.

61 Voir travaux parlementaires du projet de loi n°4889, document de dépôt p.4.

transmises »[62], ce notamment pour que le repérage ne puisse pas être confondu avec l'écoute et être vu comme une sorte de « mini-écoute ». Bien que la commission parlementaire précise que l'écoute téléphonique se fait en temps réel, notamment pour intercepter les communications et enregistrer leur contenu et que dans le cadre du repérage « *on constate simplement qu'il y a eu un appel et on essaye de localiser tant l'origine que la destination de l'appel sans qu'il soit possible d'en connaitre le contenu – ni même, comme il a déjà été relevé ci-dessus, le véritable auteur* »[63], il n'en reste pas moins que la question de savoir si l'article 67-1 du CPP pourrait servir au juge d'instruction pour ordonner une conservation des données n'a pas trouvé de réponse explicite.

67. La disposition en question autorise le juge d'instruction de procéder « *au repérage des données d'appel de moyens de télécommunication à partir desquels ou vers lesquels des appels sont adressés ou ont été adressés* »[64]. La terminologie choisie semble indiquer que le juge d'instruction peut ordonner la conservation des données qui seront encore générées. L'avis commun des Parquets du Tribunal d'Arrondissement de Luxembourg et de Diekirch[65] soutient ce point de vue. Si tel est le cas, le juge d'instruction peut donc par le biais de l'article 67-1 du CPP ordonner une conservation des données de trafic et de localisation.

68. Au vu de l'exposé de motifs, il semble que les auteurs du projet de loi n'ont pas abordé l'article sous cet angle, mais uniquement d'un point de vue d'accès aux données conservées. La CNPD se demande dès lors si l'article ne devrait pas être analysé et le cas échéant adapté afin de répondre aux exigences de la CJUE par rapport aux mesures ciblées de conservation de données.

69. Ainsi, en ce qui concerne la possibilité d'ordonner la conservation des données, l'article devra viser la finalité appropriée, contenir les conditions et critères pour délimiter l'étendue ainsi que prévoir des durées d'application et de conservation adéquates.

70. L'article 67-1 du CPP est d'ores et déjà applicable pour les faits qui emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement. La CNPD se limite à renvoyer à ses observations soulevées au points 39 à 47 du présent avis.

71. La CJUE exige encore qu'il existe dans la loi des critères permettant de limiter l'étendue des mesures de conservation. Selon la CJUE, la mesure de conservation peut être « *limitée soit sur des données afférentes à une période temporelle et/ou une zone géographique et/ou sur un cercle de personnes susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la lutte contre la criminalité grave* »[66]. Force est de constater que les modifications apportées à l'article 67-1 du CPP ne prévoient pas de tels critères, de sorte que la CNPD est à se demander si les exigences de la CJUE sont respectées.

72. La disposition sous examen contient une durée d'application de la mesure qui doit être précisée par le juge d'instruction sans qu'elle puisse excéder un mois. Or, elle néglige de fixer une durée de conservation des données de trafic et de localisation par les opérateurs et fournisseurs. Il est néanmoins essentiel de prévoir une telle durée de conservation qui doit par ailleurs être limitée au strict nécessaire par rapport au but recherché.

73. Se pose encore la question générale si la durée de conservation devrait être fixée par les dispositions qui régissent les mesures de conservation. En effet, la durée de conservation des données est une obligation qui s'adresse *in fine* aux opérateurs et aux fournisseurs. Ne serait-il dès lors pas plus logique de prévoir une disposition sur les durées de conservation des données ordonnées par les juridictions, qui seront appropriées en fonction de la mesure ordonnée dans la loi Télécom ? Dans tous

---

62 Avis du Conseil d'État du 19 mars 2002, doc. parl. n°4889/01, p.3.

63 Rapport de la Commission juridique du 2 octobre 2002, doc. parl. 4889/03, p.3.

64 Article 67-1, paragraphe 1er, point 1. du CPP dabs sa version actuelle.

65 Avis commun des Parquets du Tribunal d'Arrondissement de Luxembourg et de Diekirch du 13 avril 2023, doc. parl. n°8148/03, p.4.

66 Arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 144.

les cas, il doit découler clairement du texte que la durée de conservation s'adresse aux opérateurs et fournisseurs.

74. En dernier lieu, la CNPD se demande si une séparation des mesures de conservation et d'accès ne serait pas une alternative envisageable. Ceci dans un souci d'éviter toute confusion entre les mesures et de rendre plus lisibles les règles qui entourent ces deux mesures.

3. *La mesure de conservation du nouvel article 7-1 de la loi SRE*

75. L'article 3 point 2° du projet de loi introduit un nouvel article 7-1 dans la loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement (ci-après la « loi SRE »). Cet article permet au SRE d'ordonner aux opérateurs et fournisseurs « *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* ».

76. La CJUE admet une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation dans des situations particulières. A cet égard, elle explique que « *la sécurité nationale reste de la seule responsabilité de chaque État membre. Cette responsabilité correspond à l'intérêt primordial de protéger les fonctions essentiel/es de l'État et les intérêts fondamentaux de la société et inclut la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme* »[67]

77. La Cour admet dès lors que « *l'importance de l'objectif de sauvegarde de la sécurité nationale* […] *dépasse celle des autres objectifs visés à l'article 15, paragraphe 1, de la directive 2002/58, notamment des objectifs de lutte contre la criminalité en général, même grave, ainsi que de sauvegarde de la sécurité publique. En effet, des menaces telles que celles visées au point précédent se distinguent, par leur nature et leur particulière gravité, du risque général de survenance de tensions ou de troubles, même graves, à la sécurité publique. Sous réserve du respect des autres exigences prévues à l'article 52, paragraphe 1, de la Charte, 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* »[68].

78. Selon la CJUE, la conservation généralisée et indifférenciée des données relatives au trafic et à la localisation, qui est une ingérence particulièrement grave dans la vie privée des personnes, est donc possible si l'enjeu est la sécurité nationale. La mesure doit néanmoins être encadrée. Ainsi, la Cour considère que la menace grave doit être « *réelle et actuelle ou prévisible* »[69]. Bien que le nouvel article 7-1.1 de la loi SRE reprenne exactement ces termes, il n'est pas précisé sur base de quels critères et conditions une menace est considérée comme réelle et actuelle ou prévisible. La CNPD se demande dès lors si ces critères ne devraient pas être prévus par la loi, vu qu'une telle conservation constitue une ingérence particulièrement grave dans la vie privée des personnes concernées et qu'en vertu de l'article 52 de la Charte des droits fondamentaux de l'Union européenne (ci-après la « Charte ») et de l'article 8.2 de la Convention des droits de l'homme toute limitation de l'exercice des droits et libertés doit être prévue par la loi. Même si la CEDH admet une certaine flexibilité dans la prévisibilité de la loi en matière de surveillance secrète pour préserver la sécurité nationale[70], il n'en reste pas moins que « *[…] le risque d'arbitraire apparaît avec netteté là où un pouvoir de l'exécutif s'exerce en secret. L'existence de règles claires et détaillées en matière d'interception de conversations téléphoniques apparaît donc indispensable, d'autant que les procédés techniques utilisables ne cessent de se perfectionner. La loi doit être rédigée avec suffisamment de clarté pour indiquer à tous de manière adéquate*

---

67 Arrêt du 6 octobre 2020. La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 135.

68 *Ibid*, point 136.

69 *Ibid*, point 137.

70 Voir points 16 à 19 du présent avis.

en quelles circonstances et sous quelles conditions elle habilite la puissance publique à prendre pareilles mesures secrète »[71].

79. Aux dispositions de la Charte s'ajoutent encore celles de la Constitution. Pour rappel, ce sont en effet les droits prévus aux articles 20 (vie privée), 30 (inviolabilité des communications) et 31 (protection des données) qui sont en jeu dans le cadre du présent projet de loi. Or, conformément à l'article 37 de la Constitution « *[t]oute limitation de l'exercice des libertés publiques doit être prévue par la loi […]* ».

80. Se basant sur les constatations ci-avant, la CNPD se demande par ailleurs si la disposition est suffisamment précise quant à l'étendue de la conservation. L'utilisation de la notion « conservation généralisée et indifférenciée » ne permet pas à elle seule de savoir de quelles données, de quelles zones, de quelles personnes, voire encore de quels moyens de communication on parle. Selon sa compréhension, on entend par « conservation généralisée et indifférenciée » le stockage de toutes les données de trafic et de localisation générées par tous les moyens de communication de la quasi-totalité de la population sur tout le territoire du pays.

81. En ce qui concerne en particulier les catégories de données visées, la prévisibilité de la loi peut être remise en question. Dans le régime actuel, 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 décrit quelles données seront conservées. Les catégories de données conservées sont dès lors connues.

82. Or, comme le nouveau régime de conservation à la disposition du SRE se réfère uniquement « *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* », il ne ressort pas de manière suffisamment claire du texte de quelles données on parle exactement. La loi SRE ne contient pas de définition de ce qu'il faut entendre par une donnée relative au trafic ou à la localisation, et les définitions fournies par la loi Télécom[72] semblent également insuffisantes.

83. A l'instar de ce qu'elle a soulevé aux points 53 et 54 du présent avis, la CNPD estime qu'au moins un règlement grand-ducal devrait définir précisément quelles catégories de données constituent toutes les données de trafic et de localisation.

84. En ce qui concerne la durée de conservation, la CNPD constate à nouveau une confusion entre la durée de conservation des données et la durée d'application de la mesure. En effet, la durée de six mois prévue au nouvel article 7-1 (4) semble plutôt être une durée d'application de la mesure qu'une durée de conservation proprement dite. Il conviendrait dès lors d'ajouter une durée de conservation des données, car les opérateurs et fournisseurs doivent savoir pendant combien de temps ils doivent conserver les données une fois que la mesure prend fin.

85. L'article 7.2 de la loi SRE continue à régler l'accès aux données conservées au titre des articles 7-1 et 7-2 de la loi SRE. La CNPD se félicite qu'une référence explicite à l'article encadrant l'accès aux données soit incluse.

---

71 Voir arrêt de la CEDH du 4 décembre 2015, Roman Zakharov c. Russie, point 229.

72 Article 2 de la loi Télécom:

(...)

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

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

(...)

4. *Les mesures de conservation du nouvel article 7-2 de la loi SRE*

86. L'article 3 point 3° du projet de loi introduit un nouvel article 7-2 dans la loi SRE permettant à ce dernier d'enjoindre deux sortes de mesures : la conservation rapide et la conservation ciblée des données de trafic et de localisation.

87. Tel que soulevé aux points 31 et suivants du présent avis, les mesures de conservation rapide et de conservation ciblée ne couvrent pas les mêmes situations et ne sont pas soumises aux mêmes exigences. Il convient dès lors à apprécier les deux mesures séparément.

a. *La conservation ciblée des données de trafic et de localisation*

88. En ce qui concerne l'étendue de la mesure de conservation ciblée, la CJUE exige que la loi prévoie les critères objectifs et non discriminatoires qui permettent de déterminer les catégories de données pouvant être collectées.

89. Le projet de loi se limite à renvoyer à l'article 4 de la loi SRE qui consacre le principe général de la proportionnalité et de nécessité des mesures à prendre par le SRE. Le libellé de l'article 4 de la loi SRE ne semble en effet pas suffisamment précis pour limiter l'étendue de la mesure, car il ne fait que consacrer un principe général sans qu'il contienne des critères pour limiter la mesure de conservation ciblée à des personnes, des endroits ou des moyens de communications. Le futur article 7-2.2 de la loi SRE, quant à lui, n'en contient pas non plus comme il se limite à énoncer que l'injonction mentionne les personnes, les endroits ou encore les moyens de communications ainsi que la nature des données à conserver.

90. Au vu de la jurisprudence de la CJUE, ainsi que des exigences de la CEDH et de la Constitution tel que soulevé aux points 78 et 79 du présent avis, la CNPD estime que la loi devrait prévoir les critères pour délimiter l'étendue de la mesure de conservation.

91. Tel que déjà soulevé, notamment au point 84 du présent avis, il existe une confusion entre la durée de conservation des données et la durée d'application de la mesure. La mesure de conservation ciblée s'étend sur une certaine période pendant laquelle les opérateurs et fournisseurs sont contraints de stocker les données de trafic et de localisation. Une fois cette période venue à échéance, il convient de prévoir la durée pendant laquelle les opérateurs et fournisseurs doivent ensuite conserver les données retenues. La première période correspond à la durée d'application de la mesure, tandis que la deuxième consiste en la durée de conservation proprement dite.

92. La durée de six mois prévue au nouvel article 7-2.3 de la loi SRE semble plutôt être la durée d'application de la mesure. L'article devrait dès lors encore être complété par une durée de conservation.

b. *La conservation rapide des données de trafic et de localisation*

93. Les exigences de la CJUE quant à l'étendue de la mesure de conservation rapide sont les mêmes qu'à l'égard de la conservation ciblée. La CNPD se limite dès lors à renvoyer à ses observations aux points 88 et suivants du présent avis.

94. En ce qui concerne la durée de conservation, il convient de soulever que, contrairement à la conservation ciblée, il suffit de retenir une seule durée pour cette mesure. En effet, comme il s'agit d'une mesure ponctuelle sur des données déjà générées, il suffit de prévoir pour combien de temps les données doivent être conservées. Néanmoins, il est utile de relever que la CJUE exige qu'« *afin d'assurer que l'ingérence que comporte une mesure de ce type soit limitée au strict nécessaire, il convient, d'une part, que l'obligation de conservation porte sur les seules données de trafic et données de localisation susceptibles de contribuer à l'élucidation de l'infraction pénale grave ou de l'atteinte à la sécurité nationale concernée. D'autre part, la durée de conservation des données doit être limitée au strict nécessaire, celle-ci pouvant néanmoins être prolongée lorsque les circonstances et l'objectif*

poursuivi par ladite mesure le justifient »[73]. La CNPD se voit cependant dans l'impossibilité d'apprécier la proportionnalité de la durée retenue comme les auteurs du projet de loi n'ont pas fourni d'explications à cet égard.

95. Toujours d'après la CJUE, il est nécessaire d'inclure dans la disposition entourant la conservation rapide la finalité pour laquelle cette conservation peut avoir lieu. La CJUE explique à cet égard que « *[d]ans la mesure où la finalité d'une telle conservation rapide ne correspond plus à celles pour lesquelles les données ont été collectées et conservées initialement et où tout traitement de données doit, en vertu de l'article 8, paragraphe 2, de la Charte, répondre à des fins déterminées, les États membres doivent préciser, dans leur législation, la finalité pour laquelle la conservation rapide des données peut avoir lieu. Eu égard au caractère grave de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte qu'est susceptible de comporter une telle conservation, seule la lutte contre la criminalité grave et, a fortiori, la sauvegarde de la sécurité nationale sont de nature à justifier cette ingérence* »[74].

96. En effet, la mesure de conservation rapide cible des données qui ont déjà été générées et conservées, par exemple dans un objectif de facturation. Avec la prise d'effet de la mesure, la finalité « conservation pour des motifs de la sauvegarde de la sécurité nationale » s'ajoute à cette finalité initiale. Or, d'après la CJUE, il est nécessaire que la législation nationale prévoie cette nouvelle finalité pour les opérateurs et fournisseurs.

97. Il en est différent de la conservation ciblée qui ne prend effet que pour les données à générer dans le futur et pour lesquelles il existe dès la collecte une double finalité. Les différences non négligeables dans les exigences entourant la conservation ciblée et la conservation rapide la CNPD se pose dès lors la question, s'il ne serait pas utile de séparer les deux mesures.

B. Les mesures de conservation découlant d'une obligation légale

1. *Les mesures de conservation du nouvel article 5bis de la loi Télécom*

98. D'après la compréhension de la CNPD, le nouvel article 5*bis* entend introduire deux mesures de conservation. D'un côté, une conservation ciblée des données de trafic et de localisation délimitée sur base de zones géographiques (a). De l'autre côté, il introduit également une conservation généralisée et indifférencié (b). Comme il ne s'agit pas de mesures ponctuelles mais d'une obligation de conservation qui incombe aux opérateurs et fournisseurs dans des circonstances spécifiques, cette mesure de conservation ne doit pas être ordonnée mais découle directement de la loi.

a. *La mesure de conservation ciblée du nouvel article 5bis de la loi Télécom*

99. La mesure de conservation prévue au nouvel article 5*bis*.1 de la loi Télécom est délimitée en fonction de critères géographiques fixés au paragraphe 2 point 1° du même article. Il semble dès lors qu'il s'agit d'une mesure de conservation ciblée.

100. Pour rappel, la CJUE admet la possibilité de prévoir « *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 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 ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable* »[75]. Ainsi, la mesure de conservation doit répondre à certains critères énoncés par la CJUE.

101. Il y a lieu de constater que la disposition sous avis respecte les exigences de la CJUE en ce qui concerne la limitation des objectifs pour lesquels une conservation ciblée peut avoir lieu. Comme

---

73 Arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 164.

74 *Ibid.*

75 Arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 168.

la disposition se limite néanmoins à mentionner la « criminalité grave » sans définir, par exemple par un seuil tel que retenu au nouvel article 24-3 du CPP, ce qu'il faut entendre par cette notion, la CNPD se demande s'il ne faudrait pas apporter des précisions à cet égard.

102. En ce qui concerne la détermination des catégories de données pouvant être collectées, la CNPD renvoie à ses observations soulevées aux points 53 à 55 du présent avis.

103. Ensuite, elle constate que la limitation de l'étendue se fait sur base de certains des critères géographiques que la CJUE a proposé dans ses arrêts[76]. Ces zones seront définies par le Haut Commissariat à la protection nationale dans un arrêté grand-ducal sur proposition d'une commission consultative. La CNPD souhaite rappeler l'article 8.2 de la Convention européenne des droits de l'homme, qui prévoit qu'« *[i]l ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui* ». De plus, il y a lieu de rappeler que l'article 37 de la Constitution exige que « *[t]oute limitation de l'exercice des libertés publiques doit être prévue par la loi […]* ».

104. Concernant la condition que la mesure doit être nécessaire dans une société démocratique, la CEDH précise que des garanties adéquates et effectives doivent exister afin d'éviter l'arbitraire et les abus. Ainsi la CEDH estime que l'existence d'un contrôle de la nécessité de la mesure est une telle garantie et que l'appréciation doit se faire en prenant en compte toutes les circonstances de l'affaire en question.

105. La CNPD salue dès lors les observations du Conseil d'État formulées à l'encontre de l'arrêté grand-duca1[77] en particulier parce que le commentaire des articles précise que l'étendue du périmètre de chaque zone sera fixée par arrêté grand-ducal qui ne sera pas publié obligatoirement. De plus, comme la commission consultative n'a qu'un rôle de conseil et que son avis n'est pas contraignant pour le Haut-Commissariat à la protection nationale, la CNPD se demande comment le contrôle de la nécessité sera effectué. Sans aucun autre moyen de contrôle effectif, la CNPD considère la publication comme un aspect important dans le cadre du contrôle de la nécessité d'une mesure.

106. En ce qui concerne la revue des zones géographiques, le commentaire des articles indique à juste titre que la CJUE exige que les zones doivent être adaptables notamment lorsque les conditions ayant justifié la conservation changent[78]. La CNPD s'interroge cependant quant à la période de 3 ans retenue pour effectuer cette revue. Les auteurs du projet de loi n'expliquent pas pourquoi ce délai semble approprié de sorte qu'il est impossible d'apprécier ce choix. De plus, la CNPD estime qu'il faudrait prévoir une procédure permettant une revue anticipée au cas où les conditions changent de manière à justifier l'adaptation du périmètre de la zone, voire l'abandon de la surveillance dans une certaine zone.

107. Toujours à l'égard de l'étendue de la mesure, le paragraphe 3 de l'article 5*bis* entend introduire l'obligation pour les opérateurs et fournisseurs de continuer de conserver les données de trafic et de localisation des personnes en déplacement, c'est-à-dire des personnes qui au moment d'une communication entrent ou sortent d'une telle zone. La CNPD peut comprendre l'intention des auteurs du projet de loi, mais elle souhaite néanmoins mettre en garde qu'une telle obligation ne doit pas aboutir à une conservation généralisée et indifférenciée sur la quasi-totalité de la population et sur la totalité du territoire. La conservation doit rester l'exception.

108. L'article 5*bis*.1 fixe une durée de conservation des données de six mois à partir de la communication. Le commentaire des articles se limite à justifier ce choix par le « *souci d'unification et*

---

76 Voir arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791 et arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258.

77 Voir avis du Conseil d'État du 23 janvier 2024, doc. parl. 8148/05, p.8.

78 Voir par exemple arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 82.

d'harmonisation des durées de conservation ». La CNPD est d'avis que cette justification n'est pas suffisante pour apprécier la proportionnalité de la durée retenue.

109. De plus, l'article 5*bis* dans sa rédaction actuelle ne contient pas d'indication ou de référence vers la ou les dispositions encadrant l'accès aux données conservées. La CNPD rappelle que l'accès ne peut se faire que dans le respect de la hiérarchie des objectifs. En effet, la CJUE explique que les données conservées pour l'objectif de la sécurité nationale ne peuvent pas être accédées pour des finalités de lutte contre la criminalité grave[79]. L'inverse semble pourtant légitime[80]. Comme l'article sous avis concerne la conservation pour deux objectifs, à savoir la lutte contre la criminalité grave et la préservation de la sécurité nationale, la précision quant aux articles réglant les accès pourrait s'avérer utile. La séparation des mesures en deux articles distincts pourrait également faciliter la compréhension des accès.

b. *La mesure de conservation généralisée et indifférenciée du nouvel article 5bis de la loi Télécom*

110. Le nouvel article 5*bis*.2 point 2° instaure l'obligation pour les opérateurs et fournisseurs de conserver les données de trafic et de localisation de manière généralisée et indifférenciée 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* ».

111. La CNPD tient à rappeler que la conservation généralisée et indifférenciée des données de trafic et de localisation n'est possible que pour des objectifs de la sauvegarde de la sécurité nationale. Or, comme le premier paragraphe de l'article énonce également l'objectif de la lutte contre la criminalité grave, une certaine incertitude quant à la finalité de la conservation généralisée et indifférenciée reste. Même si l'on peut s'imaginer que les conditions qui déclencheraient cette conservation, à savoir que le niveau de la menace soit au niveau 3 au plan VIGILNAT et couvre l'ensemble du territoire, sont en lien avec l'objectif de la sécurité nationale, ceci ne ressort pas clairement du texte. La CNPD se demande dès lors s'il ne serait pas utile de séparer les deux mesures et clarifier qu'une telle conservation généralisée et indifférenciée ne peut se faire que pour l'objectif de la sécurité nationale. Ceci également au vu du respect de la hiérarchie des objectifs expliquée au point 109 du présent avis.

112. Concernant l'étendue de la mesure, et notamment les catégories de données visées, la CNPD n'a pas d'autres observations que celles qu'elle a déjà soulevées aux points 53 à 55 du présent avis, à savoir qu'il doit ressortir clairement de la législation quelles données sont susceptibles d'être collectées.

113. Sans précision quant au moment qui déclenche la durée de la mesure de conservation, la CNPD estime que c'est l'information du Haut-Commissariat à la protection nationale. Le texte ne prévoit pourtant ni une durée de la mesure, ni une procédure pour revoir la nécessité de la mesure ou pour mettre fin à la collecte au cas où elle ne serait plus nécessaire. La CNPD se demande dès lors si le principe de nécessité est respecté à cet égard.

114. Tel que mentionné au point 108 du présent avis, la CNPD se trouve dans l'impossibilité d'apprécier la durée de conservation retenue.

115. Enfin, la CNPD souhaite réitérer ses observations à l'égard de l'utilité d'une référence vers la ou les dispositions encadrant l'accès aux données conservées.

---

79 Voir arrêt du 20 septembre 2022, SpaceNet et Telekom Deutschland C-793/19 et c-794/19, EU:C:2022:702, point 128.
80 *Ibid.*

2. La mesure de conservation du nouvel article 10ter.1 de la loi Télécom

116. Tel qu'expliqué par le commentaire des articles, la CJUE reconnait la possibilité pour les États membres de prévoir une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques. Ceci notamment parce que « *ces données ne permettent pas, à elles seules, de connaitre 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* »[81]. Il en résulte que l'ingérence dans la vie privée ne peut pas être qualifiée de grave[82].

117. Selon le commentaire des articles, « *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* ». Ainsi, l'article 10*ter*.1 ne serait qu'un complément de l'article 10*bis*. Si tel est le cas, la CNPD ne comprend pas pourquoi l'article 10*bis* n'a pas été adapté, d'autant plus que ce dernier contient des références aux articles permettant l'accès aux données conservées.

118. De plus, le point 1° de l'article 10*ter* impose aux opérateurs et fournisseurs de conserver les données qu'ils détiennent au titre de l'article 10*bis*. Est-ce que cette obligation n'est pas superfétatoire du simple fait que les opérateurs et fournisseurs ont déjà cette obligation et qu'un accès à ces données est régi par l'article 10*bis* ? L'interaction entre les deux articles ne semble pas tout à fait claire et prête à confusion.

119. Ensuite, la CNPD s'interroge sur l'utilisation du verbe « générer » dans la partie introductive du paragraphe 1er, ceci notamment en lien avec la collecte des données détenues sur base de l'article 10*bis* ainsi que l'IMEI[83] et l'IMSI[84]. Est-ce que les opérateurs et fournisseurs sont tenus de générer ces données pour leurs abonnés et/ou utilisateurs ? Ou est-ce qu'ils doivent également conserver les données de l'article 10*bis* (nom, prénom, lieu de résidence…etc.), l'IMSI et l'IMEI des destinataires de la communication (par exemple l'appelé) ? Il ne ressort pas clairement du texte que ces données se réfèrent uniquement à l'abonné/l'utilisateur. Au cas où non seulement les données des abonnées/utilisateurs, mais également celles des destinataires de la communication devront être conservées, la CNPD se demande si cette conservation n'irait pas au-delà des limites posées par la CJUE.

120. Par ailleurs, la CNPD constate que certaines notions utilisées dans cet article ne sont pas définies. Il est dès lors incertain ce que l'article vise concrètement. Premièrement, les notions de « données de souscription » et « données d'identification » ne sont pas définies. Il est donc impossible de savoir de quelles données il est question. La notion d'« utilisateur final » n'est pas non plus définie. Est-ce que l'on vise ici la définition retenue dans l'article 2, point 14° de la loi du 17 décembre 2021 sur les réseaux et les services de communications électroniques? Enfin, les notions d'« adresses IP ayant servi à la souscription ou à l'activation » ainsi que « le port de source » mériteraient d'être définies afin de savoir quelles données seront collectées concrètement.

121. Vu que la disposition manque de clarté par rapport aux données qui seront traitées, ainsi qu'en ce qui concerne l'interaction avec l'article 10*bis*, la CNPD n'est pas en mesure d'apprécier si les données conservées ne sont pas « *susceptibles de permettre de tirer des conclusions précises, voire très*

---

81 Voir arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 157.

82 *Ibid.*

83 Selon le commentaire des articles, l'IMEI « *est un numéro d'identification unique qui permet d'immatriculer un équipement mobile* ».

84 Selon le commentaire des articles, l'IMSI « *est un identifiant qui se trouve dans la carte SIM et qui permet d'identifier de manière unique chaque abonné* ».

précises, concernant la vie privée des personnes dont les données ont été conservées »[85] tel que l'exige la CJUE.

3. *La mesure de conservation du nouvel article 10*ter.*2 de la loi Télécom*

122. D'après la CJUE, « *la conservation généralisée et indifférenciée des seules adresses IP attribuées à la source d'une connexion n'apparaît pas, en principe, contraire à l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des article 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, pourvu que cette possibilité soit soumise au strict respect des conditions matérielles et procédurales devant régir l'utilisation de ces données* »[86]. La Cour ajoute encore qu'« *[e]u égard au caractère grave de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte que comporte cette conservation, 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* »[87].

123. Il y a lieu de constater que la disposition sous avis semble respecter les exigences de la CJUE en ce qui concerne la limitation des objectifs pour lesquels une conservation ciblée peut avoir lieu. Comme la disposition se limite néanmoins à mentionner la « criminalité grave » sans définir, par exemple par un seuil tel que retenu au nouvel article 24-3 du CPP, ce qu'il faut entendre par cette notion, la CNPD se demande s'il ne faudrait pas apporter des précisions à cet égard.

124. A cet égard, il faut prendre en compte la récente jurisprudence de la CJUE qui n'existait pas encore au moment du dépôt du projet de loi sous avis. Il s'agit de l'arrêt du 30 avril 2024. La Quadrature du Net e.a. (Données personnelles et lutte contre la contrefaçon), qui contient des observations[88] quant à la possibilité de prévoir une conservation généralisée et indifférenciée des adresses IP attribuées à la source aux fins d'objectifs de lutte contre les infractions pénales en général.

125. La Cour apporte des précisions à sa position soulevée au point 122 du présent avis, et explique qu'elle « *s'est expressément fondée, pour parvenir à cette conclusion, sur Je caractère grave de l'ingérence dans les droits fondamentaux consacrés aux articles 7, 8 et 11 de la Charte qu'est susceptible de comporter une telle conservation des adresses IP* »[89]. Elle ajoute que l'ingérence grave dérive du fait qu'il est possible d'effectuer un traçage exhaustif du parcours de navigation de la personne concernée ou d'établir le profil détaillé. D'après la Cour un tel profilage ou traçage n'est possible que si les différentes informations conservées, dont les adresses IP, sont combinées. Grâce à cette combinaison, il est dès lors possible de tirer des conclusions précises sur la vie privée des personnes concernées[90].

126. Il apparaît donc que ce n'est pas nécessairement la conservation généralisée et indifférenciée des adresses IP attribuées à la source qui constitue une ingérence grave dans la vie privée des personnes concernées, mais plutôt la possibilité de combiner ces données avec d'autres données collectées. La CJUE précise dès lors que « *l'obligation faite aux fournisseurs de services de communications électroniques, par une mesure législative au titre de l'article 15, paragraphe 1, de la directive 2002158, d'assurer la conservation généralisée et indifférenciée des adresses IP peut, le cas échéant, être justifiée par l'objectif de la lutte contre les infractions pénales en général lorsqu'il est effectivement exclu que cette conservation puisse engendrer des ingérences graves dans la vie privée de la personne concernée en raison de la possibilité de tirer des conclusions précises sur celle-ci moyennant, notamment, une mise en relation de ces adresses IP avec un ensemble de données de trafic ou de localisation qui auraient également été conservées par ces fournisseurs* »[91].

---

85 Voir arrêt du 2 octobre 2018, Ministerio Fiscal C-207/16, EU:C:2018:788, point 60.

86 Voir arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 155.

87 *Ibid*, point 156.

88 Voir arrêt du 30 avril 2024, La Quadrature du Net e.a. (Données personnelles et lutte contre la contrefaçon), C-470/21, EU:C:2024:370, points 66 à 94.

89 *Ibid*., point 77.

90 *Ibid*., points 78 à 80.

91 *Ibid*., point 82.

127. La Cour en déduit qu'un « *Etant membre qui entend imposer aux fournisseurs de services de communications électroniques une obligation de conservation généralisée et indifférenciée des adresses IP en vue d'atteindre un objectif lié à la lutte contre les infractions pénales en général doit s'assurer que les modalités de conservation de ces données soient de nature à garantir qu'est exclue toute combinaison desdites adresses IP avec d'autres données conservées, dans le respect de la directive 2002/58, qui permettrait de tirer des conclusions précises sur la vie privée des personnes dont les données seraient ainsi conservées* »[92].

128. La Cour exige en effet une séparation stricte entre les différentes catégories de données conservées. Cette exigence fait penser à l'image de plusieurs coffres-forts qui contiennent les différentes catégories de données et qui empêchent que les données puissent être reliées entre eux. La Cour ajoute encore que la législation nationale doit prévoir « *des règles claires et précises relatives auxdites modalités de conservation, ces modalités devant répondre à des exigences strictes* »[93].

129. Aux points 86 à 89, la CJUE fournie des précisions quant à ces modalités. Il faut ainsi que les données soient conservées séparément, et que sur un plan technique cette séparation soit étanche. Une troisième exigence de la Cour consiste en la mise en place d'un procédé technique performant qui effectue la mise en relation entre les adresses IP et les données d'identité civile conservée, ceci dans un objectif de préserver la séparation étanche. En dernier lieu, la CJUE exige que la séparation étanche fasse l'objet d'un contrôle régulier par une autorité publique. La CJUE conclut que lorsque ces modalités sont respectées et qu'il n'est pas possible de combiner des données pour tirer des conclusions précises sur la vie privées des personnes concernées, une conservation généralisée et indifférenciée des adresses IP aux fins d'un objectif de lutte contre les infractions pénales en général est possible.

130. Au vu de ce qui précède, la CNPD estime que la disposition sous examen devrait être revue pour respecter la récente jurisprudence de la CJUE.

131. De plus, faute de fournir des explications dans le commentaire des articles quant au choix de la durée de conservation retenue, la CNPD se trouve dans l'impossibilité de l'apprécier.

132. Enfin, il y a lieu de soulever que le terme « port » utilisé à la fin du premier alinéa prête à confusion. De quoi s'agit-il exactement ? Est-ce qu'il s'agit des mêmes « ports source de la connexion » mentionnés au paragraphe 1er ? Dans l'affirmative, ne faudrait-il pas aligner la terminologie ?

C. Les garanties entourant la conservation par les opérateurs et fournisseurs

133. Bien que les mesures de conservation doivent être accompagnées de garanties en ce qui concerne la possibilité d'y avoir recours, la CJUE exige également que la conservation en elle même par les opérateurs et fournisseurs soit entourée de garanties contre les risques d'abus et d'accès illicites.

134. La CJUE explique en effet que « *compte tenu de la quantité importante de données relatives au trafic et de données de localisation susceptibles d'être conservées de manière continue par une mesure de conservation généralisée et indifférenciée ainsi que du caractère sensible des informations que ces données peuvent fournir, la seule conservation desdites données par les fournisseurs de services de communications électroniques comporte des risques d'abus et d'accès illicite* »[94].

135. Ainsi, la Cour exige notamment que les opérateurs et fournisseurs détruisent de manière irrémédiable les données à la fin de la durée de conservation[95], qu'ils conservent les données sur le territoire de l'Union[96], qu'ils assurent la pleine intégrité et la confidentialité desdites données et garantissent un niveau particulièrement élevé de protection et de sécurité par des mesures techniques et

92 *Ibid*., point 83.

93 *Ibid*., point 85.

94 Voir arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 119.

95 Voir arrêt du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 67.

96 *Ibid*., point 68.

organisationnelles appropriées. Par ailleurs, elle exige que les États membres garantissent un contrôle, par une autorité indépendante, du respect du niveau de protection garanti par le droit de l'Union en matière de protection des personnes physiques à l'égard du traitement des données à caractère personnel[97].

136. En l'occurrence, c'est l'article 2 points 3° et 8° du projet de loi qui est intéressant à cet égard comme il modifie les articles 5 et 9 de la loi Télécom.

137. Concernant la destruction irrémédiable préconisée par la CJUE, la CNPD constate que tant la version modifiée de l'article 5 que celle de l'article 9 de la loi Télécom prévoient que les données de trafic et de localisation sont supprimées ou rendues anonymes « *dès lors qu'elles ne sont plus nécessaires à la transmission d'une communication* ». Il existe des exceptions à cette suppression, notamment à l'article 5.2 et 5.3 de la loi Télécom, qui semblent admissibles et ne soulèvent pas d'observations particulières de la part de la CNPD. Cependant, les articles 5.1 et 9.1 de la loi Télécom prévoient une autre exception qui, a priori, semble logique mais qui mériterait néanmoins d'être précisée.

138. En effet, l'article 9.1 prévoit que les données de trafic et de localisation sont supprimées lorsqu'elles ne sont plus nécessaires à la transmission d'une communication « *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* ». La rédaction de l'article 5.1 est similaire.

139. La CNPD se demande si cette partie de la phrase doit être comprise comme la conséquence logique de la possibilité pour certaines autorités de demander la conservation des données aux opérateurs et fournisseurs. En d'autres termes, est-ce qu'il s'agit d'une simple confirmation du principe que des mesures de conservation peuvent être mises en place ? Si tel est le cas, il convient néanmoins de s'interroger sur les termes utilisés. Il n'est effectivement pas clair pourquoi l'article dispose que « *[…] à l'exception des accès qui sont ordonnés par les autorités judiciaires et par le comité ministériel du renseignement […]* ». Ne devrait-on pas plutôt écrire « à l'exception des données dont la conservation a été ordonnée […] » ?

140. La rédaction actuelle laisse effectivement un doute quant à la suppression des données dont la conservation a été ordonnée, enjointe ou prévue par un texte légal, et qui par la suite ont été accédées par les autorités compétentes. Si la lecture de l'article devait être telle que les données qui ont été accédées ne seront pas supprimées, ceci serait contraire à la jurisprudence de la CJUE.

141. De plus, la CNPD considère qu'il faudrait prévoir une durée de conservation maximale de ces données. Ceci notamment par rapport à ce qui a été soulevé dans le présent avis pour plusieurs mesures de conservation, à savoir qu'il ne ressort pas clairement des dispositions pendant combien de temps les données doivent être conservées par les opérateurs et fournisseurs comme il y a un mélange entre durée d'application de la mesure et durée de conservation des données[98].

142. Concernant la limitation des accès aux personnes strictement nécessaires, les futurs articles 5.4 et 9.4 de la loi Télécom semblent refléter cette exigence de la CJUE. Un contrôle par une autorité indépendante compétente en matière de protection des données est également prévu.

143. Il convient néanmoins de se demander pourquoi les auteurs du projet de loi n'ont pas inclus les autres exigences de la CJUE à savoir que les opérateurs et fournisseurs doivent conserver les données sur le territoire de l'Union et assurer la pleine intégrité et la confidentialité desdites données, et garantir un niveau particulièrement élevé de protection et de sécurité par des mesures techniques et organisationnelles appropriées.

---

97 Voir arrêt du 21 décembre 2016, Tele2 Sverige et Watson e. a., C-203/15 et C-698/15, EU:C:2016:970, point 123.

98 Voir par exemple points 58 et 59 du présent avis.

144. En dernier lieu, il faut constater qu'aucune mesure de conservation ne contient des garanties envers les personnes soumises au secret professionnel au sens de l'article 458 du Code pénal ainsi que les lanceurs d'alerte. La CJUE explique en effet que « *la conservation des données relatives au trafic et des données de localisation à des fins policières est susceptible, à elle seule, de porter atteinte au droit au respect des communications […] et d'entraîner des effets dissuasifs sur l'exercice par les utilisateurs des moyens de communications électroniques de leur liberté d'expression, garantie à l'article 11 de [la Charte]. Or, de tels effets dissuasifs peuvent affecter en particulier les personnes dont les communications sont soumises, selon les règles nationales, au secret professionnel ainsi que les lanceurs d'alerte […]. En outre, ces effets sont d'autant plus graves que le nombre et la variété des données conservées sont élevés* »[99]. La CNPD regrette dès lors que les auteurs du projet de loi n'aient pas prévu des garanties à l'égard de ces catégories de personnes.

*

II. Les mesures législatives d'accès aux données

145. Une fois les données conservées, il est nécessaire de prévoir un deuxième ensemble de mesures autorisant les autorités compétentes à accéder les informations. La CJUE explique clairement qu'elle considère que l'accès par les autorités compétentes aux données conservées constitue une ingérence supplémentaire dans la vie privée des personnes concernées[100].

146. Ainsi, et comme les mesures d'accès correspondent, tout comme les mesures de conservations, à une dérogation au principe de confidentialité, elles doivent également respecter les exigences de la CJUE[101].

147. Les mesures d'accès doivent dès lors « *être subordonnées à des garanties appropriées* »[102] et ainsi « *prévoir des règles claires et précises indiquant en quelles circonstances et sous quelles conditions les fournisseurs de services de communications électroniques doivent accorder aux autorités nationales compétentes l'accès aux données. De même, une mesure de cette nature doit être légalement contraignante en droit interne* »[103]. La Cour ajoute encore qu'« *une telle réglementation nationale doit également prévoir les conditions matérielles et procédurales régissant l'accès des autorités nationales compétentes aux données conservées* »[104].

148. La jurisprudence de la Cour fournit des indications sur ce qu'une mesure législative d'accès doit contenir. Elle exige par exemple que la législation contienne des critères afin de limiter le nombre de personnes ayant accès aux données[105]. Elle considère par ailleurs « *qu'un accès général à toutes les données conservées, indépendamment d'un quelconque lien, à tout le moins indirect, avec le but poursuivi, ne saurait être considéré comme limité au strict nécessaire* »[106]. Il est dès lors essentiel que la loi contienne « *des critères objectifs pour définir les circonstances et les conditions dans lesquelles doit être accordé aux autorités nationales compétentes l'accès aux données des abonnés ou des utilisateurs inscrits. À cet égard, un accès ne saurait, en principe, être accordé, en relation avec l'objectif de lutte contre la criminalité, qu'aux données de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction grave ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction […].* »[107].

---

99 Voir arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 118.

100 Voir arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 116 et arrêt du 2 octobre 2018, Ministerio Fiscal C-207/16, EU:C:2018:788, point 51.

101 Voir arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 165.

102 Voir arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 117.

103 *Ibid*.

104 *Ibid*., point 118.

105 Voir arrêt du 8 avril 2014, Digital Rights Ireland e.a., C-293/12 et C-594/12, EU:C:2014:238, point 62.

106 Voir arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 119.

107 *Ibid*.

149. Ainsi, outre l'exigence que seulement les personnes strictement nécessaires aient accès aux données, la Cour exige que la loi fixe des critères et conditions déterminant dans quels cas les données peuvent être accédées. De plus, la CJUE demande qu'il existe un lien au moins indirect entre l'objectif de lutte contre la criminalité et la personne dont les données seront accédées. Pour cette dernière exigence, la Cour admet néanmoins une atténuation en cas de menace par des activités terroristes. Dans ce cas, il suffit que des éléments objectifs permettent de démontrer que les informations accédées puissent contribuer à la lutte contre de telles activités[108].

150. En ce qui concerne les objectifs des mesures d'accès, la jurisprudence de la CJUE répète à plusieurs reprises que dans le respect de la hiérarchie des objectifs, l'accès aux données « *ne peut en principe être justifié que par l'objectif d'intérêt général pour lequel cette conservation a été imposée à ces fournisseurs. Il n'en va autrement que si l'importance de l'objectif poursuivi par l'accès dépasse celle de l'objectif ayant justifié la conservation* »[109]. Ainsi, quand des données ont été conservées pour des objectifs de sauvegarde de la sécurité nationale, elles ne peuvent pas être accédées pour des objectifs de lutte contre la criminalité grave. L'inverse serait cependant admissible.

151. D'un point de vue procédural, la CJUE exige que la mesure d'accès fasse l'objet d'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 présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénales* »[110].

152. La CJUE n'admet le contrôle postérieur qu'en cas d'urgence dûment justifiée. Le contrôle doit alors intervenir dans les plus brefs délais[111]. La Cour explique à cet égard qu'un « *contrôle ultérieur ne permettrait pas de répondre à l'objectif d'un contrôle préalable, consistant à empêcher que soit autorisé un accès aux données en cause qui dépasse les limites du strict nécessaire* »[112].

153. Une garantie supplémentaire contre les risques d'abus que la CJUE juge importante est « *que les autorités nationales compétentes auxquelles l'accès aux données conservées a été accordé, en informent les personnes concernées, dans le cadre des procédures nationales applicables, des le moment où cette communication n'est pas susceptible de compromettre les enquêtes menées par ces autorités* »[113]. Ainsi, les mesures législatives doivent prévoir une telle information des personnes concernées qui est effectivement nécessaire pour leur permettre d'exercer leurs droits en matière de protection des données.

154. Enfin, la CJUE soulève que la transmission par les opérateurs et fournisseurs de données de trafic et de localisation aux autorités répressives entraine des « *effets dissuasifs sur l'exercice par les utilisateurs des moyens de communications électroniques de leur liberté d'expression, garantie à l'article 11 de la Charte. De tels effets dissuasifs peuvent affecter en particulier les personnes dont les communications sont soumises, selon les règles nationales, au secret professionnel ainsi que les lanceurs d'alerte* »[114]. Il serait dès lors souhaitable qu'une mesure législative d'accès prévoit des garanties à l'égard des personnes soumises au secret professionnelles ainsi que des lanceurs d'alerte.

155. A la lecture du projet de loi, il devient clair qu'il existe quatre mesures législatives qui régissent les accès aux données conservées. Trois de ces mesures sont prévues dans le Code de procédure pénale, notamment aux articles 48-27 du CPP (1) et l'article 67-1 du CPP (2) et une est prévue par l'article 7.2 de la loi SRE (3). Il convient dès lors de voir si les différentes mesures d'accès respectent les exigences de la CJUE décrites ci-avant.

---

108 *Ibid*.

109 Voir arrêt du 20 septembre 2022 SpaceNet et Telekom Deutschland C-793/19 et c-794/19, EU:C:2022:702, point 128.

110 Voir arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 120.

111 Voir arrêt du 2 mars 2021, Prokuratuur, C-746/18, EU:C:2021:152, point 58.

112 *Ibid*.

113 Voir arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 190.

114 Voir arrêt du 6 octobre 2020, Privacy International, C-623/17, EU:C:2020:790, point 72.

A. Les mesures d'accès sur base de l'article 48-27 du Code de procédure pénale

156. L'article 1er point 2° du projet de loi entend remplacer l'article 48-27 du CPP et ajoute une nouvelle mesure d'accès à la mesure d'accès aux données d'identification (1) déjà prévue à cet article. En effet, le nouveau paragraphe 2 de l'article 48-27 du CPP introduit une mesure d'accès relative aux données IP (2). Comme ces deux mesures doivent répondre à des exigences différentes, il est nécessaire de les examiner séparément.

1. *La mesure d'accès aux données d'identification sur base de l'article 48-27.1 du Code de procédure pénale*

157. Le projet de loi entend adapter la rédaction de l'article 48-27 du CPP pour refléter les changements de la loi Télécom, notamment l'introduction de l'article 10*ter*.1 qui prévoit l'obligation légale pour les opérateurs et fournisseurs de conserver les données d'identification des utilisateurs. Ainsi, l'article 48-27.1 du CPP dans sa rédaction nouvelle attribuera la possibilité au juge d'instruction et au procureur d'État d'accéder à ces données d'identification.

158. En ce qui concerne les objectifs pour lesquels un accès aux données conservées est possible, il y a lieu de constater que la disposition sous avis ne limite pas l'applicabilité à des infractions spécifiques. Ainsi, le recours à cette mesure d'accès est possible tant pour la sauvegarde de la sécurité nationale que pour la lutte contre la criminalité grave ainsi que pour la lutte contre la criminalité en général.

159. Dans l'arrêt Ministerio Fiscal de 2018[115], la CJUE a pu se prononcer sur une telle mesure d'accès aux seules données d'identification. Elle clarifie en particulier la question de savoir pour quels objectifs [sécurité nationale, criminalité grave, criminalité simple) un accès aux seules données d'identification est possible.

160. Il ressort clairement de cet arrêt que la Cour détermine la gravité de l'ingérence dans la vie privée des personnes concernées en fonction de la nature des données accédées. Ainsi, lorsque sont accédées des données qui ne permettent pas de tirer des conclusions précises concernant la vie privée des personnes concernées, l'ingérence n'est pas qualifiée de grave. Dans le cas concret de l'arrêt Ministerio Fiscal, les données permettaient « *uniquement de mettre en relation, pendant une période déterminée* [12 jours]*, la ou les cartes SIM activées avec le téléphone mobile volé avec l'identité civile des titulaires de ces cartes SIM. Sans un recoupement avec les données afférentes aux communications effectuées avec lesdites cartes SIM et les données de localisation, ces données ne permettent de connaitre ni la date, l'heure, la durée et les destinataires des communications effectuées avec la ou les cartes SIM en cause, ni les endroits où ces communications ont eu lieu ou la fréquence de celles-ci avec certaines personnes pendant une période donnée* ». La Cour conclut par dire que si l'accès vise donc des données d'identité civile, c'est-à-dire le nom, prénom, et le cas échéant l'adresse, ainsi que les seuls numéros de téléphone correspondant à ces cartes SIM, cette ingérence ne peut pas être qualifiée de grave.

161. Dans le même arrêt, la CJUE soulève que « *lorsque l'ingérence que comporte un tel accès n'est pas grave, ledit accès est susceptible d'être justifié par un objectif de prévention, de recherche, de détection et de poursuite d'« infractions pénales » en général* ». Il en résulte que, pour autant qu'elles ne permettent pas de tirer de conclusions précises concernant la vie privée des personnes concernées, l'accès aux données permettant l'identification des utilisateurs est possible pour les objectifs de sauvegarde de la sécurité nationale, de lutte contre la criminalité grave ainsi que de lutte contre la criminalité en général.

162. Au vu de ce qui précède, la disposition sous avis semble en conformité avec la jurisprudence de la CJUE, mais uniquement dans la mesure où elle ne vise effectivement que l'accès aux données

---

115 Voir arrêt du 2 octobre 2018, Ministerio Fiscal C-207/16, EU:C:2018:788, points 48 à 63.

aux fins d'identification des utilisateurs. Vu la rédaction actuelle de l'article, la CNPD se pose plusieurs questions.

163. Premièrement, il convient de s'interroger sur la partie de phrase « *sur la base de toutes données détenues par lui sur base de l'article 10ter, paragraphe 16 de la loi modifiée du 30 mai 2005* » du 1er paragraphe de l'article 48-27 du CPP. Au vu de ce qui a été soulevé dans la partie I.B.2 et en particulier au point 119 du présent avis, la CNPD se demande si on ne vise réellement que des données d'identification ou si cela va au-delà. Dans ce dernier cas, la disposition ne serait pas conforme à la jurisprudence de la CJUE.

164. Deuxièmement, la CNPD émet également des doutes quant à l'étendue du point 2° du paragraphe 1er en ce qu'il prévoit un accès à des fins d'« *identification des services de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée* ». Est-ce qu'une telle identification des services utilisés n'irait pas au-delà de ce qui est autorisé par la CJUE qui fait explicitement référence à la possibilité d'accéder aux données à des fins d'identification des utilisateurs ?

165. Si l'accès visé à l'article 48-27.1 du CPP serait plus large et qu'il viserait également des données qui doivent être considérées comme des données de trafic et de localisation, alors l'accès devrait être considéré comme permettant de tirer des conclusions précises concernant la vie privée des personnes concernées. L'ingérence devrait dès lors être qualifiée de grave et un accès ne pourrait être possible que pour les objectifs de préservation de la sécurité nationale et de lutte contre la criminalité grave.

166. Ensuite, en ce qui concerne l'exigence de la CJUE qu'« *un accès ne saurait, en principe, être accordé, en relation avec l'objectif de lutte contre la criminalité, qu'aux données de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction grave ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction* »[116], la CNPD constate que le projet de loi ne la prévoit pas expressément. Elle estime qu'il appartient au juge d'instruction ou au procureur d'État de justifier l'existence d'un tel lien entre la personnes concernée et l'objectif poursuivi dans la décision motivée et écrite mentionnée dans l'article 48-27.1 du CPP. La CNPD se demande néanmoins s'il ne faudrait pas modifier le texte à cet égard.

167. Par ailleurs, il y a lieu de constater que la mesure d'accès aux données d'identité civile ne contient pas la garantie de l'information des personnes concernées par les autorités compétentes que leurs données ont été accédées. Dans la mesure où la CJUE exige l'existence d'une telle garantie, la CNPD estime que la disposition devrait être complétée.

168. Enfin, la CNPD regrette que l'article 48-27 du CPP ne contienne pas de garanties à l'égard des personnes soumises au secret professionnel ainsi que les lanceurs d'alerte.

2. La mesure d'accès aux données d'identification sur base de l'article 48-27.2 du Code de procédure pénale

169. Ensuite, le projet de loi entend introduire une nouvelle mesure d'accès à l'article 48-27.2 du CPP, à savoir la possibilité d'accéder, sur décision du procureur d'État ou du juge d'instruction et à des fins d'identification de l'utilisateur, aux données IP conservées au titre du nouvel article 10*ter*.2 de la loi Télécom.

170. Il convient de rappeler que la jurisprudence récente de la CJUE doit être prise en considération pour cette mesure, à savoir l'arrêt du 30 avril 2024, précité La Quadrature du Net e.a. (Données personnelles et lutte contre la contrefaçon) en particulier les points 95 à 122. Cet arrêt apporte des précisions, par rapport aux exigences auxquelles une disposition législative prévoyant l'accès aux adresses IP conservées doit répondre, y compris en ce qui concerne le contrôle préalable.

---

116 Voir arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 119.

171. En ce qui concerne les exigences auxquelles une mesure d'accès aux adresses IP attribuées à la source doit répondre, et spécifiquement les objectifs pour lesquelles un tel accès peut être décidé, la Cour opère un lien avec ses observations sur la conservation de telles données. Ainsi, la Cour estime que la conservation séparée et étanche des données constitue le prérequis pour que l'accès aux adresses IP attribuées à la source pour des infractions dites simples soit possible. Ceci notamment pour garantir que l'ingérence dans la vie privée des personnes reste la moins intrusive possible dans la mesure où aucun traçage ou profilage ne soit possible du fait que les données puissent être combinées.

172. En revanche, la Cour indique que seule la finalité de l'identification justifierait un accès aux adresses IP dans le cadre de la lutte contre la criminalité dite simple et que la mesure législative doit contenir des garanties contre des abus. Elle ajoute encore, qu'il faut toujours respecter le principe de la hiérarchie des objectifs.

173. La CNPD considère en conséquence que la disposition sous examen doit être revue afin de respecter cette jurisprudence. Elle se félicite par ailleurs que la mesure ne peut être prise qu'aux seules fins d'identification. En effet, toute utilisation à d'autres fins semble non-conforme à la jurisprudence de la CJUE.

174. Néanmoins, en ce qui concerne l'exigence de la CJUE qu'« *un accès ne saurait, en principe, être accordé, en relation avec l'objectif de lutte contre la criminalité, qu'aux données de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction grave ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction* »[117], la CNPD constate que le projet de loi ne la prévoit pas expressément. Elle renvoie à cet égard à ces observations soulevées au point 166 du présent avis.

175. La CNPD se demande encore pourquoi cette mesure est régie par l'article 48-27 du CPP et non pas par l'article 67-1 du CPP, notamment au regard de l'exigence de la CJUE de la nécessité d'un contrôle indépendant préalable pour l'accès à des données de trafic ou de localisation.

176. En effet, la CJUE explique qu'« *il est essentiel que l'accès des autorités nationales compétentes aux données conservées soit 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 présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénales* »[118]. Elle poursuit en soulevant que « *l'exigence d'indépendance à laquelle doit satisfaire l'autorité chargée d'exercer le contrôle préalable […] impose que cette autorité ait la qualité de tiers par rapport à celle qui demande l'accès aux données, de sorte que la première soit en mesure d'exercer ce contrôle de manière objective et impartiale à l'abri de toute influence extérieure* »[119]. La Cour soutient encore que « *[t]el n'est pas le cas d'un ministère public qui dirige la procédure d'enquête et exerce, le cas échéant, l'action publique* [120] et conclut que « *le ministère public n'est pas en mesure d'effectuer le contrôle préalable* »[121].

177. D'après la compréhension de la CNPD, le procureur d'État ne devrait dès lors pas être en mesure d'enjoindre une telle mesure d'accès. Cette possibilité ne devrait être attribuée qu'au seul juge d'instruction.

178. De plus, il convient de souligner que la CJUE admet la possibilité d'accéder aux données de trafic et de localisation sans autorisation préalable mais ce uniquement en cas d'urgence dûment justifiée. Dans cette situation, le contrôle doit néanmoins intervenir dans des brefs délais. Une telle procédure d'urgence est prévue à l'article 48-27.3 du CPP. La CNPD constate néanmoins que la disposition ne contient pas de délai endéans duquel le contrôle doit être effectué. Elle se demande s'il ne faudrait pas prévoir un délai maximal suffisamment court pour être conforme à la jurisprudence de la CJUE.

---

117 Voir arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 119.

118 Voir arrêt du 2 mars 2021, Prokuratuur, C-746/18, EU:C:2021:152, point 51.

119 *Ibid*., point 54.

120 *Ibid*., point 57.

121 *Ibid*.

179. Encore faut-il soulevé que la jurisprudence récente de la CJUE admet une atténuation à cette position[122]. En effet, en admettant la conservation et l'accès des adresses IP attribuées à la source dans le cadre de la lutte contre la criminalité dite simple à des fins d'identification, la Cour ne manque pas de se prononcer sur le contrôle préalable par une juridiction ou une autorité administrative indépendante dans ce contexte. Ainsi, la Cour souligne que « *dans le cas où un dispositif de conservation tel que celui décrit aux points 86 à 89 du présent arrêt est mis en place, l'accès de l'autorité publique aux données relatives à l'identité civile correspondant aux adresses IP ainsi conservées n'est, en principe, pas subordonné à l'exigence d'un contrôle préalable par une juridiction ou par une entité administrative indépendante* »[123] Il convient donc également de revoir, le cas échéant, la disposition sous examen, afin de respecter les observations de la CJUE.

180. Concernant la garantie des personnes concernées d'être informées de l'accès à leurs données à caractère personnel, la CNPD renvoie à ses observations soulevées au point 167 du présent avis.

181. Enfin, la CNPD regrette que l'article 48-27 du CPP ne contienne pas de garanties à l'égard des personnes soumises au secret professionnel ainsi que les lanceurs d'alerte.

B. La mesure d'accès sur base de l'article 67-1 du Code de procédure pénale

182. Selon le commentaire des articles, l'article 67-1 du CPP dans sa rédaction nouvelle « *vise l'accès des autorités judiciaires aux données relatives au trafic et de localisation, conservées par les opérateurs et fournisseurs concernés conformément aux dispositions inscrites à la Loi Telecom ainsi que désormais au titre du nouvel article 24-3 du Code de procédure pénale proposé par le présent projet de loi* ».

183. Ainsi, l'intention des auteurs du projet de loi semble être que le juge d'instruction peut ordonner non seulement l'accès aux données conservées pour des motifs de lutte contre la criminalité grave, mais également pour les besoins de sauvegarde de la sécurité nationale au titre de l'article 5*bis* de la loi Télécom.

184. Elle note néanmoins que l'article 67-1 du CPP ne semble viser que les situations où « *les faits emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement* ».

185. A cet égard, la CNPD souhaite rappeler que conformément au principe de la hiérarchie des objectifs, l'accès aux données conservées « *ne peut en principe être justifié que par l'objectif d'intérêt général pour lequel cette conservation a été imposée à ces fournisseurs. Il n'en va autrement que si l'importance de l'objectif poursuivi par l'accès dépasse celle de l'objectif ayant justifié la conservation* »[124]. Il en résulte que des données conservées, par exemple pour des motifs de sauvegarde de la sécurité nationale, ne peuvent pas être accédées pour des objectifs de lutte contre la criminalité grave.

186. La CNPD est consciente du fait que la terminologie « *les faits emportent une peine criminelle ou une peine correctionnelle dont le maximum est égal ou supérieur à un an d'emprisonnement* » semble a priori également comprendre les infractions qui mettent en péril la sécurité nationale. Il convient néanmoins de s'interroger comment, en pratique, la distinction entre un accès aux données conservées pour des motifs de lutte contre la criminalité grave et un accès aux données conservées pour les besoins de sauvegarde de la sécurité nationale s'opère.

187. Ou bien faut-il lire l'article 67-1 du CPP de manière à ce que le juge ne puisse pas ordonner un accès aux données conservées pour les besoins de sauvegarde de la sécurité nationale ? Dans ce cas, ne priverait-on pas le juge d'instruction d'une mesure nécessaire dans le cadre de l'instruction ?

---

122 Voir arrêt du 30 avril 2024, La Quadrature du Net e.a. (Données personnelles et lutte contre la contrefaçon), C-470/21, EU:C:2024:370, en particulier les points 123 à 151.

123 *Ibid*., point 134.

124 Voir arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 98.

188. Est-ce que la rédaction de l'article 67-1 du CPP ne devrait pas être revue afin de s'assurer que le juge d'instruction ait toutes les mesures d'accès nécessaires à sa disposition, tout en respectant le principe de la hiérarchie des objectifs ?

189. En ce qui concerne les critères objectifs pour définir les circonstances et les conditions dans lesquelles les autorités nationales compétentes peuvent obtenir accès aux données conservées, les auteurs du projet de loi indiquent dans le commentaire des articles que « *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 » ». Selon les auteurs du projet de loi, cette condition semble suffisante pour répondre aux exigences de la CJUE.

190. La CNPD se demande pourtant si la disposition sous avis répond avec suffisance à l'exigence qu'il existe un « *lien, à tout le moins indirect, avec le but poursuivi, ne saurait être considéré comme limité au strict nécessaire* »[125]. La CJUE exige que la législation prévoie l'existence d'un lien au moins indirect entre l'objectif de lutte contre la criminalité et la personne dont les données seront accédées. Pour cette dernière exigence, la Cour admet néanmoins une atténuation en cas de menace par des activités terroristes. Dans ce cas il suffit que des éléments objectifs permettent de démontrer que les informations accédées puissent contribuer à la lutte contre de telles activités[126]. Elle renvoie à cet égard à ses observations soulevées au point 166 du présent avis.

191. Par ailleurs, concernant l'exigence « *que les autorités nationales compétentes auxquelles l'accès aux données conservées a été accordé, en informent les personnes concernées, dans le cadre des procédures nationales applicables, dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes menées par ces autorités* »[127], la CNPD se félicite que le projet de loi conserve cette garantie supplémentaire contre les risques d'abus.

192. La CNPD se demande néanmoins comment cette garantie est mise en œuvre dans la pratique. Comment les personnes qui, in fine, ne font pas l'objet d'une procédure pénale sont informées ? Est-ce que toutes les personnes sont informées, à savoir la personne ciblée ainsi que les personnes avec lesquelles cette dernière était en correspondance ?

193. Enfin, la CNPD regrette que l'article 67-1 du CPP ne contienne pas de garanties à l'égard des personnes soumises au secret professionnel ainsi que les lanceurs d'alerte.

C. La mesure d'accès sur base de l'article 7.2 de la loi SRE

194. Bien que le projet de loi n'entende apporter que des modifications mineures à l'article 7 de la loi SRE, la CNPD estime nécessaire de soulever quelques observations étant donné qu'il régit l'accès du SRE à des données de trafic et de localisation.

195. Ainsi, la CNPD se pose notamment la question si l'article 7 de la loi SRE régit également l'accès de ce dernier aux données d'identification conservées au titre de l'article 10*ter* de la loi Télécom. La partie de phrase « *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* » semble indiquer que tel est le cas. La CNPD estime néanmoins que des précisions, par exemple sous forme de renvoi, pourraient servir à la lisibilité et à la compréhension de la mesure d'accès.

196. Ensuite, il y a lieu de constater que la mesure d'accès aux données ne contient pas la garantie de l'information des personnes concernées par les autorités compétentes que leurs données ont été accédées. Dans la mesure où la CJUE exige l'existence d'une telle garantie, la CNPD se demande s'il ne faudrait pas compléter l'article 7 de la loi SRE.

---

125 Voir arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15, EU:C:2016:970, point 119.

126 *Ibid*.

127 Voir arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 190

197. Enfin, la CNPD se félicite que les auteurs du projet de loi ont maintenu dans l'article 7.3 alinéa 5 une garantie pour les données de « *personnes liées par le secret professionnel au sens de l'article 458 du Code pénal et non suspectes elles-mêmes d'être impliquées dans une menace actuelle ou potentielle relevant du champ d'application des missions du SRE déterminés à l'article 3* »[128]. En effet, cette garantie répond au moins en partie aux risques exprimés par la CJUE que la transmission par les opérateurs et fournisseurs de données de trafic et de localisation aux autorités répressives entraine des « *effets dissuasifs sur l'exercice par les utilisateurs des moyens de communications électroniques de leur liberté d'expression, garantie à l'article 11 de la Charte. De tels effets dissuasifs peuvent affecter en particulier les personnes dont les communications sont soumises, selon les règles nationales, au secret professionnel ainsi que les lanceurs d'alerte* »[129].

*

III. LES AUTRES DISPOSITIONS MODIFICATIVES

A. L'alignement de la définition du consentement à celle retenue par le RGPD

198. L'article 2 point 1° du projet de loi vise selon le commentaire des articles à aligner la définition du terme « consentement » de la loi Télécom à celle utilisée dans le RGPD. La CNPD constate néanmoins qu'il ne s'agit pas d'une reprise fidèle de la définition et s'interroge sur cette adaptation.

B. Les modifications apportées à l'article 5-1 de la loi Télécom (désormais article 5*ter* de la loi Télécom)

199. La CNPD s'interroge sur la plus-value du paragraphe 1er. En effet, la disposition prévoit que « *[l]es données conservées au titre des articles 5, 5bis et 9 de la présente loi par les autorités compétentes au sens de l'article 18 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* ». Dans la mesure où la loi précitée 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 s'applique de toute manière aux traitements effectués par ces autorités pour autant que le traitement ait lieu à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces, la CNPD ne comprend pas la raison d'être de cette disposition.

200. De plus, il convient de s'interroger sur la rédaction du paragraphe 2 en ce qu'il prévoit que « *[l]es 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* ». Est-ce que cette disposition s'applique aux autorités compétentes, c'est-à-dire aux autorités qui ont accédé ou auxquelles les données ont été transmises, ou est-ce qu'elle s'applique aux opérateurs et fournisseurs ? Il convient encore de se demander comment cette disposition interagit avec les autres dispositions contenant des durées de conservation. Enfin, la partie de phrase « *à l'exception des données auxquelles on a pu légalement accéder et qui ont été préservées* » suscite des interrogations de la part de la CNPD, étant donné que cette exception semble impliquer que certaines données n'ont pas de durée de conservation maximale. La CNPD estime dès lors que ce paragraphe mérite d'être clarifié.

*

---

128 Loi modifiée du 5 juillet 2016 portant réorganisation du Service de renseignement de l'État, article 7 paragraphe 3 alinéa 5.

129 Voir arrêt du 6 octobre 2020, Privacy International, C-623/17, EU:C:2020:790, point 72.

IV. OBSERVATIONS SUPPLEMENTAIRES

201. La CNPD saisit l'occasion du projet de loi de soulever que pour des violations en matière de protection des données de la loi Télécom elle n'est actuellement pas en mesure de recourir à ses pouvoirs découlant de l'article 58 du RGPD. Elle suggère dès lors fortement au législateur de prévoir une disposition afin d'étendre les compétences et pouvoirs de la CNPD à l'égard de la loi Télécom. Ainsi, elle propose, par exemple, de compléter l'article 12 de la loi Télécom par un deuxième paragraphe avec une teneur similaire de l'article 12 de la loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données :

> *« (2) Dans le cadre des missions conférées par le paragraphe 18 la CNPD dispose des pouvoirs prévus à l'article 58 du règlement (UE) 2016/679. »*

202. De plus, la CNPD souhaite soulever que deux dispositions de la loi Télécom ne semblent plus en adéquation avec la législation actuelle concernant la protection des données, étant donné que le RGPD est entré en application en 2018 et que la loi Télécom date de 2005.. Il s'agit d'un côté des paragraphes 3 à 5 de l'article 3 de la loi Télécom qui traitent des violations de données à caractère personnel, et plus particulièrement des notifications à faire à la CNPD, de l'inventaire à tenir ainsi que de la sanction pénale en cas de manquement aux obligations. Le RGPD connaît un régime spécifique pour les violations des données à caractère personnel qui diffère dans certains points à celui prévu par la loi Télécom. Ainsi, le régime du RGPD ne connaît pas, par exemple, de sanction pénale. De plus, la CNPD ne comprend pas ce qui justifie que le régime des notifications de violations de la loi Télécom reste différent de celui prévu par le RGPD, notamment par rapport aux acteurs du terrain qui doivent se conformer à ces deux régimes. Elle suggère dès lors d'aligner la loi Télécom à ce qui est prévu par le RGPD en remplaçant les trois paragraphes par une référence aux dispositions pertinentes du RGPD.

203. De l'autre côté, il s'agit de l'article 4(3)(e) de la loi Télécom qui prévoit une dérogation au principe de confidentialité lorsque l'abonné ou l'utilisateur a donné son consentement. Il importe de soulever que le RGPD a défini le consentement comme « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement* ». Les termes importants de cette définition sont « *par une déclaration ou par un acte positif clair* ». Il faut dès lors que la personne concernée ait donné son consentement de manière explicite. Le recueil implicite du consentement n'est plus valable[130]. Or, la rédaction actuelle de l'article 4(3)(e) et en particulier la dernière phrase de ce point[131] rend possible le recueille implicite du consentement.

204. Il importe de soulever qu'il ressort de la guidance du Comité européen pour la protection des données que l'article 95 du RGPD implique qu'« *[a]ussi les conditions d'obtention d'un consentement valable établies par le RGPD sont-elles applicables dans les situations tombant dans le champ d'application de la directive «vie privée et communications électroniques* » »[132]. La CNPD note encore que la volonté des auteurs du projet de loi d'aligner la définition de consentement dans la loi Télécom avec celle du RGPD démontre que ce terme doit être compris de la même manière. La CNPD estime donc essentiel que cette dernière phrase de l'article 4(3)(e) de la loi Télécom soit supprimée.

---

130 Ainsi, par exemple, un site ne peut plus afficher des cases déjà cochées pour recueillir le consentement. Il faut que la personne concernée coche la case lui-même.

131 Article 4(3)(e) dernière phrase de la loi Télécom : « *Lorsque cela est techniquement possible et effectif, l'accord de l'abonné ou de l'utilisateur peut être exprimé par l'utilisation des paramètres appropriés d'un navigateur ou d'une autre application* ».

132 Voir les lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/769 du comité européen pour la protection des données point 7.

Ainsi adopté à Belvaux en date du 16 mai 2024.

La Commission nationale pour la protection des données

Tine A. LARSEN
Présidente

Thierry LALLEMANG
Commissaire

Marc LEMMER
Commissaire

Alain HERRMANN
Commissaire

Impression: CTIE – Division Imprimés et Fournitures de bureau