Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 66/2022 du 1er avril 2022

Objet : Demande d'avis concernant 18 amendements modifiant le projet de loi relatif à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités (CO-A-2022-057)

Le Centre de Connaissances de l'Autorité de protection des données (ci-après « l'Autorité »),
Présent : Monsieur Bart Preneel ;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26 (ci-après « LCA ») ;

Vu le règlement (UE) 2016/679 *du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (ci-après « RGPD ») ;

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après « LTD ») ;

Vu la demande d'avis du Vice-premier Ministre et Ministre de la Justice et de la Mer du Nord, Vincent Van Quickenborne, reçue le 1er mars 2022 ;

émet, le 1er avril 2022, l'avis suivant :

I. OBJET ET CONTEXTE DE LA DEMANDE D'AVIS

1. Le Vice-premier Ministre et Ministre de la Justice et de la Mer du Nord a sollicité l'avis de l'Autorité concernant **18 amendements modifiant le projet de loi relatif à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités** (ci-après « les amendements »).

2. Le projet de loi relatif à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités (ci-après « **le projet de loi de réparation de la loi *data retention*** » ou « **projet de loi de réparation** ») fait suite à l'annulation, par la Cour constitutionnelle, dans son arrêt n° 57/2021 du 22 avril 2021, « *des articles 2, b), 3 à 11 et 14 de la loi du 29 mai 2016 'relative à la collecte et à la conservation des données dans le secteur des communications électroniques'* » (ci-après « **la loi du 29 mai 2016** »).

3. Cette loi du 29 mai 2016 prévoyait, comme le rappelle la lettre envoyée à l'Autorité par le demandeur, « *l'obligation pour les fournisseurs au public de services de téléphonie, en ce compris par internet, d'accès à l'Internet et de courrier électronique par Internet (qu'ils soient opérateurs notifiés à l'IBPT ou non) de conserver certaines catégories de données de localisation et de trafic pendant une durée de 12 mois essentiellement afin que ces données soient disponibles pour des finalités répressives (enquêtes pénales) ou pour l'accomplissement des missions des services de renseignement et de sécurité* ». Cette loi de 2016 imposait ainsi une obligation de conservation généralisée et indifférenciée de certaines données de trafic et de localisation, mais ne concernait pas le contenu des communications. Elle a été annulée par la Cour constitutionnelle en raison de sa contrariété avec l'article 15 de la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (ci-après « la Directive ePrivacy »), lu à la lumière des articles 7 et 8, ainsi que de l'article 52 § 1 de la Charte des droits fondamentaux de l'Union européenne, en combinaison avec les articles 10 et 11 de la Constitution. L'annulation de la Cour constitutionnelle est très largement motivée par un renvoi à l'arrêt que la Cour de justice de l'Union européenne (ci-après « la CJUE ») a rendu à la suite des questions préjudicielles posées, notamment, par la Cour constitutionnelle concernant l'interprétation à donner à l'article 15 de la Directive ePrivacy[1].

4. À la suite de cet arrêt, **le Gouvernement a préparé un projet de loi de réparation de la *loi data retention* sur lequel l'Autorité s'est prononcée dans son avis n° 108/2021 du 28 juin 2021**.

[1] CJUE, arrêt du 6 octobre 2020, aff. Jointes C-511/18, C-512/18 et C-520/18 (affaire dite de « La Quadrature du Net »). Cet arrêt de la CJUE a été rendu à la suite, notamment, des questions préjudicielles posées par la Cour constitutionnelle dans son arrêt n° 96/2018 du 19 juillet 2018.

5. Le 18 novembre 2021, la Cour constitutionnelle a annulé « *l'article 2 de la loi du 1er septembre 2016 'portant modification de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité', uniquement en ce qu'il ne détermine pas les données d'identification qui sont collectées et traitées et les documents d'identification qui entrent en considération* ». Dans cet arrêt n° 158/2021, la Cour constitutionnelle a, en effet, jugé que « *l'article 127 de la loi du 13 juin 2005, tel qu'il a été modifié par l'article 2 de la loi attaquée, viole le principe de légalité garanti par l'article 22 de la Constitution, mais seulement en ce qu'il ne détermine pas les données d'identification qui sont collectées et traitées et les documents d'identification qui entrent en considération* »[2]. En d'autres termes, **la Cour constitutionnelle** a rappelé, dans cet arrêt, que le **principe de légalité** consacré par l'article 22 de la Constitution **impose au législateur de déterminer, lui-même, les données et les documents d'identification** qui doivent être conservées par les opérateurs, étant donné que ces données et documents d'identification constituent un élément essentiel du traitement de données à caractère personnel.

6. Pour rappel, le principe de légalité consacré par l'article 22 de la Constitution vise à garantir *« à tout justiciable qu'aucune ingérence dans l'exercice [du droit à la vie privée] ne peut avoir lieu qu'en vertu de règles adoptées par une assemblée délibérante, démocratiquement élue. Une délégation au pouvoir exécutif n'est toutefois pas contraire au principe de légalité, pour autant que l'habilitation soit définie de manière suffisamment précise et qu'elle porte sur l'exécution de mesures dont les éléments essentiels ont été fixés préalablement par le législateur* ». Les **données et documents d'identification** qui doivent être conservés par les opérateurs télécom constituent, selon la Cour constitutionnelle, un **élément essentiel** qui **doit être déterminé par le législateur lui-même**, et ne peut être délégué au pouvoir exécutif.

7. À la suite de l'arrêt n° 158/2021, le Gouvernement estime que certaines dispositions du projet de loi de réparation devaient être revues. Les **amendements soumis pour avis entendent, notamment, répondre à cet arrêt** et garantir que les dispositions du 13 juin 2005 relative aux communications électroniques (ci-après « la loi télécom »), telles qu'elles seront modifiées par le projet de loi de réparation, qui imposent aux opérateurs de conserver certaines données (qu'il s'agisse de données de souscription de l'abonné, de données d'identification de l'abonné ou encore de données de trafic ou de localisation) respectent le principe de légalité formelle.

8. Bien que l'arrêt de la Cour constitutionnelle n° 158/2021 ne porte que sur l'article 127 de la loi télécom, il ressort de l'analyse effectuée par le Gouvernement que d'autres dispositions, en particulier les articles 126 et 126/1 de la loi télécom, doivent également être revues afin d'y énumérer les données qui doivent être conservées par les opérateurs.

[2] Considérant B.9.1 de l'arrêt

9. L'**amendement n° 1** vise ainsi à **remplacer l'article 126** de la loi télécom qui impose aux opérateurs de conserver les **données de souscription** de l'abonné ainsi que les **données techniques** qui sont nécessaires **pour identifier** l'utilisateur final, l'équipement terminal ou le service de communications électroniques employé, si et dans la mesure où l'opérateur traite ou génère ces données. La nouvelle version de l'article 126 liste les données qui doivent être conservées par les opérateurs pour autant qu'ils les traitent ou les génèrent dans le cadre de la fourniture des réseaux communications électroniques ou des services de communications électroniques.

10. Les **amendements n° 2 et 3** visent à insérer dans la loi télécom les métadonnées de communications électroniques, en ce compris les métadonnées pour les appels infructueux, auxquelles s'appliquent l'obligation de conservation imposée par le **nouvel article 126/1,** qui sera inséré dans la loi télécom par le projet de loi de réparation. Ces métadonnées de communications électroniques seront énumérées dans **un nouvel article 126/2** de la loi télécom.

11. L'**amendement n° 4** vise à adapter **l'article 145** de loi télécom, de sorte que le non-respect de l'arrêté royal d'exécution de l'article 126/2 soit puni par l'amende pénale prévue à l'article 145. L'**amendement n° 5** vise à ajouter un article 39 au projet de loi de réparation afin de donner aux opérateurs un délai d'un an pour conserver les « nouvelles données », à savoir des données visées dans les nouveaux articles 126 et 126/2 de la loi télécom et qui ne sont pas prévues dans l'arrêté royal du 19 septembre 2013 portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques.

12. L'**amendement n° 6** vise à remplacer **l'article 127** dans la loi télécom qui impose aux opérateurs **d'identifier ses abonnés au moyen d'une méthode d'identification directe** (qui doit être utilisée, en principe, pour les services de communications électroniques payants) **ou d'une des méthodes d'identification indirecte** qu'il liste (lesquelles doivent être utilisées pour les services de communications électroniques gratuits et qui doivent aussi être utilisées, dans certains cas, pour des services de communications électroniques payants).

13. L'**amendement n° 7** vise à insérer un nouvel **article 127/4** dans la loi télécom qui reprend une interdiction qui était auparavant reprise à l'article 127 § 2 de la loi télécom. L'**amendent n° 8** vise à adapter **l'article 145** de la loi télécom afin de veiller à ce que le non-respect du nouvel article 127/4 de la loi télécom (inséré par l'amendement n° 7) soit puni par une amende pénale. L'**amendement n° 9**, qui introduit un article 40 dans le projet de loi de réparation, vise (1) à clarifier que les modifications apportées à l'article 127 de la loi télécom ne s'appliqueront que pour les contrats conclus après l'entrée en vigueur de la loi, (2) à laisser un délai de 24 mois aux opérateurs avant qu'ils ne soient tenus d'accepter tous les documents d'identités listés par le nouvel article 127 (ce délai doit leur permettre d'adapter leurs systèmes) et (3) à laisser aux opérateurs un délai de 24 mois avant qu'ils ne

soient tenus de collecter les nouvelles données « minimales » qu'ils doivent collecter en vertu du nouvel article 127.

14. Les **amendements 10 à 15** visent à **modifier la loi du 17 janvier 2003** relative au statut du régulateur des secteurs des postes et des télécommunications belges (ci-après « la loi IBPT ») afin de déterminer les conditions dans lesquelles **l'IBPT peut avoir accès aux données d'identifications, de trafic et de localisation conservées par les opérateurs.**

15. Un amendement non numéroté – mais identifions-le comme **l'amendement n° 16** – vise à modifier **l'article 46bis du Code d'instruction criminelle** (ci-après « C.I.C ») afin de donner explicitement au Procureur du Roi le pouvoir de requérir, afin d'obtenir l'identification de l'abonné ou de l'utilisateur final d'un service de communications électroniques, la collaboration des banques et des institutions financières (sur la base de la référence d'une transaction bancaire électronique qui lui a été préalablement communiquée), des centres fermés ou lieu d'hébergement (pour étrangers) (sur la base des coordonnées du centre ou du lieu d'hébergement où la souscription de l'abonné à un service de communications électroniques mobiles a été effectuée et qui lui a été préalablement communiquées), des autres personnes morales qui sont abonnées ou souscrivent à un service de communications électroniques au nom et pour le compte de personnes physiques (sur la base des données qui lui ont préalablement été communiquées par un opérateur).

16. Un amendement non numéroté – mais identifions-le comme **l'amendement n° 17** – vise à modifier **l'article 11 § 1er de la loi du 24 janvier 1977** relative à la protection de la santé des consommateurs en ce qui concerne les denrées alimentaires et les autres produits (ci-après « la loi du 24 janvier 1977 ») afin de permettre au service d'inspection Produit de la consommation de requérir la collaboration des banques et des institutions financières, sur la base de la référence d'une transaction électronique qui a préalablement été communiquée par un opérateur, afin que le service d'inspection puisse procéder à l'identification de la personne concernée.

17. Un amendement non numéroté – mais identifions-le comme **l'amendement n° 18** – vise à modifier **l'article 81 de la loi du 2 août 2002** relative à la surveillance du secteur financier et aux services financiers (ci-après « la loi du 2 août 2002 ») afin de permettre à l'auditeur (ou l'auditeur adjoint) de l'Autorité des services et marchés financiers (ci-après « la FSMA ») de requérir, pour obtenir l'identification de l'abonné ou de l'utilisateur final du service, la collaboration des banques et des institutions financières (sur la base de la référence d'une transaction bancaire électronique qui lui a été préalablement communiquée), des centres fermés ou lieu d'hébergement (pour étrangers) (sur la base des coordonnées du centre ou du lieu d'hébergement où la souscription de l'abonné à un service de communications électroniques mobiles a été effectuée et qui lui a été préalablement communiquées), des autres personnes morales qui sont abonnées ou souscrivent à un service de

communications électroniques au nom et pour le compte de personnes physiques (sur la base des données qui lui ont préalablement été communiquées par un opérateur).

18. Le demandeur a demandé que l'Autorité examine en urgence ces amendements. L'Autorité entend souligner qu'au vu de l'impact important des amendements sur les droits et libertés de l'ensemble des personnes résidant en Belgique et y utilisant des moyens de communications électroniques, soit la quasi-totalité de la population, **il n'est pas acceptable qu'elle ne dispose ni du temps ni des ressources nécessaires pour analyser le dossier dans les meilleures conditions**. Exceptionnellement, malgré ses moyens insuffisants au regard de sa charge de travail[3], **l'Autorité rend son avis dans les meilleurs délais**. Elle invite le demandeur à anticiper, à l'avenir, au mieux ses demandes d'avis dans cette matière qui a un impact significatif sur les droits et libertés des citoyens et des citoyennes.

19. Avant d'examiner les amendements soumis pour avis à la lumière du droit à la protection des données à caractère personnel, l'Autorité rappelle que, **dans son avis n° 108/2021**, elle a émis de **nombreuses remarques**, certaines étant tout à fait fondamentales, à propos du projet de loi de réparation de la loi *data retention*. L'Autorité insiste sur le fait que **le projet de loi de réparation doit réellement opérer le changement de perspective** exigé par la jurisprudence de la CJUE et de la Cour constitutionnelle et qu'il ne peut donc pas imposer de nouvelles mesures de conservation des données de trafic et de localisation qui aboutiraient à réintroduire, *de jure ou de facto*, des obligations de conservation des données de trafic ou de localisation de l'ensemble ou d'une proportion trop importante des utilisateurs de moyens de communications électroniques en Belgique. Or l'Autorité a constaté, dans son avis n° 108/2021, que l'avant-projet de loi qui lui avait été soumis pour avis n'opérait pas complètement ce changement de perspective puisque puisqu'il entendait imposer de nouvelles mesures de conservation des données de trafic et de localisation (afin de lutter, notamment, contre la fraude, l'utilisation malveillante du réseau et pour garantir la sécurité des réseaux) qui pourraient aboutir à réintroduire, *de facto*, des obligations de conservation généralisée et indifférenciée des données. **À défaut de revoir en profondeur le projet de loi de réparation afin de s'assurer qu'il opère le changement de perspective exigé, tant la conservation de ces données de trafic et de localisation par les opérateurs que leur communication aux autorités porteraient atteinte à la directive ePrivacy, interprétée à la lumière des articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne**. Or une nouvelle annulation par la Cour constitutionnelle de la loi de réparation serait de nature à entacher gravement la confiance des citoyennes et les citoyens dans les institutions démocratiques.

[3] À ce propos, l'Autorité souligne, comme elle l'a déjà fait dans l'annexe à l'avis sur l'avant-projet de loi portant modification de la loi APD, que **la charge de travail du Centre de connaissances a plus que triplé ces dernières années** (75 avis rendus en 2017 et 249 en 2021) alors que les **ressources humaines affectées au Centre de connaissances ont diminué** (13 juristes étaient affectés à la rédaction d'avis en 2018 alors que cette tâche est accomplie par 8 juristes actuellement). Début avril 2022, le Centre de connaissances avait déjà rendu 65 avis ; ce qui augure une nouvelle augmentation exponentielle de la charge de travail pour cette année 2022.

20. **L'Autorité insiste pour que le législateur respecte les exigences issues du droit à la protection des données à caractère personnel lorsqu'il adoptera le projet de loi de réparation. À cette fin, l'Autorité renvoie à l'avis n° 108/2021 pour tous les aspects qui ne sont pas couverts dans le présent avis**. Par ailleurs, l'Autorité relève déjà qu'elle ne formulera, en principe, des remarques à propos des amendements qui lui sont soumis pour avis que dans la mesure où celles-ci apparaissent nécessaires au vu des nouveaux éléments apportés par les amendements et leur justification.

II. EXAMEN DE LA DEMANDE D'AVIS

21. Dans son avis, l'Autorité va examiner ci-dessous **les amendements n° 1, 2, 3, 6, 7, 12, 15, 16, 17 et 18**, étant donné que les autres amendements n'appellent pas de commentaire au regard du droit à la protection des données à caractère personnel.

22. Mais avant d'examiner, dans le détail, ces amendements à la lumière des exigences découlant du droit à la protection des données à caractère personnel, telles qu'elles ressortent de l'article 22 de la Constitution, des articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, de la directive ePrivacy et du RGPD, l'Autorité émet une **remarque préalable** sur l'extension du **champ d'application** de la *data retention* et de l'obligation d'identification des abonnés et des utilisateurs finaux.

A. Remarque préalable sur l'extension du champ d'application de la *data retention* et de l'obligation d'identification des abonnés et des utilisateurs finaux

23. En transposant le Code de communications électroniques européen (ci-après « CCEE ») dans la loi télécom[4], **le législateur a redéfinit, entre autres, les notions d'« *opérateur* »[5] et de « *services de communications électroniques* »[6]**, qui sont utilisées pour déterminer le champ d'application personnel des obligations imposées aux opérateurs de conserver les données de trafic et de localisation des abonnés et de l'obligation d'identification des abonnés et des utilisateurs finaux des services de communications électroniques. Comme l'Autorité l'a déjà soulevé dans son avis n° 108/2021, **ces nouvelles définitions aboutissent à étendre considérablement le champ**

[4] Cette transposition a eu lieu par l'adoption de la loi du 21 décembre 2021 portant transposition du code des communications électroniques européen et modification de diverses dispositions en matière de communications.
[5] Cette notion est définie comme « *une personne ou entreprise qui fournit un réseau public de communications électroniques ou un service de communications électroniques accessible au public* » (article 2, 11° de la loi télécom)
[6] Cette notion est définie comme « *le service fourni normalement contre rémunération via des réseaux de communications électroniques qui, à l'exception des services consistant à fournir des contenus transmis à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ces contenus et à l'exception des services de médias audiovisuels ou sonores, comprend les types de services suivants :*
a) un service d'accès à l'internet ;
b) un service de communications interpersonnelles ; et
c) des services consistants entièrement ou principalement en la transmission de signaux, tels que les services de transmission utilisés pour la fourniture de services de machine à machine ».

d'application des obligations de conservation des données et d'identification des abonnés et utilisateurs finaux. Avec la transposition du CCE dans la loi télécom, les entreprises qui fournissent des services de communications électroniques « over-the-top », à l'instar de services de téléphonie par Internet *(Voice over IP)*, de services de messageries (p.ex. : WhatsApp, Signal, Telegram, Facebook Messenger), ou encore de services de courrier électroniques en ligne (p.ex. : Gmail ou Hotmail) sont soumises à des obligations de conservation de données et doivent procéder à l'identification de leurs abonnés ou utilisateurs finaux. De même, les entreprises qui fournissent des « *services consistants entièrement ou principalement en la transmission de signaux, tels que les services de transmission utilisés pour la fourniture de services de machine à machine* »[7] – il s'agit de services portant sur l'internet des objets – doivent, à présent, être considérées comme des opérateurs soumis à des obligations de conservation des données et à l'obligation d'identifier leurs abonnés et utilisateurs finaux.

24. Ainsi, les nouvelles définitions des notions d'« opérateur » et de « services de communications électroniques », couplées, notamment, à l'obligation d'identification imposée par les nouveaux articles 126 et 127 de la loi télécom (introduits par les amendements n° 1 et 6), **aboutissent à rendre impossible – ou en tout cas très difficile – toute correspondance anonyme sur Internet**. En outre, pour les services de messagerie « OTT » (comme Signal ou WhatsApp), l'Autorité relève que la collecte et la conservation des adresses IP attribuées à la source de la connexion permet, non seulement d'identifier de manière indirecte l'utilisateur, mais également (potentiellement) de le localiser. En effet, il est souvent possible de localiser un équipement terminal (et donc la personne qui l'utilise) à partir de l'adresse IP qui lui a été attribuée. La collecte systématique des adresses IP attribuées à la source de la connexion et leur horodatage permettent ainsi potentiellement de suivre les déplacements des utilisateurs de ces services ; ce qui constitue une ingérence particulièrement importante dans le droit au respect de la vie privée de ces utilisateurs.

25. Ceci constitue un changement de paradigme par rapport au paradigme de, et aux règles de confidentialité imposées par, la directive ePrivacy[8]. **L'Autorité insiste sur la nécessité de tenir un débat parlementaire approfondi sur les implications de ce changement, notamment, au regard du droit à la vie privée et du droit à la liberté d'expression[9]. En tout état de cause,**

[7] L'Autorité s'interroge sur la portée potentiellement très large de cette définition alors que la loi télécom ne définit pas ce qu'il faut entendre par « *services consistants entièrement ou principalement en la transmission de signaux, tels que les services de transmission utilisés pour la fourniture de services de machine à machine* ».

[8] En effet, voyez, à ce sujet, l'observation de la CJUE dans l'arrêt du 6 octobre 2020 : « […] les internautes disposent, conformément à ce qui a été constaté au point 109 du présent arrêt, du droit de s'attendre, en vertu des articles 7 et 8 de la Charte, à ce que leur identité ne soit, en principe, pas dévoilée […] » (§ 155)

[9] Quand bien même, l'obligation d'identification des utilisateurs d'un service de communications électroniques n'interfère pas directement avec le droit à la liberté d'expression, l'Autorité relève que cette obligation pourrait avoir un « **chilling effect** » (c'est-à-dire un « effet dissuasif » ou « effet inhibiteur ») sur l'exercice du droit à la liberté d'expression par le biais de moyens de communications électroniques. L'existence d'un tel effet dissuasif sur l'exercice d'un droit ou d'une liberté fondamentale peut être qualifiée, aux termes de la jurisprudence de la CJUE ou de la CEDH, comme une ingérence dans le droit ou cette liberté (en l'occurrence, le droit à la liberté d'expression). Sur la reconnaissance du fait que l'adoption de mesure ayant un effet dissuasif sur l'exercice d'un droit ou d'une liberté fondamentale constitue une ingérence dans l'exercice de ce doit, voyez

l'Autorité rappelle que toute ingérence dans les droits et libertés des personnes concernées n'est admissible que si elle s'avère nécessaire et proportionnée à l'objectif d'intérêt général poursuivi.

B. Concernant l'amendement n° 1

26. L'amendement n° 1 prévoit de **remplacer l'article 126 dans la loi télécom**. Cette disposition entend **imposer aux opérateurs** qui offrent aux utilisateurs finaux des services de communications électroniques, ainsi qu'aux opérateurs fournissant les réseaux de communications électroniques qui permettent la fourniture de ces services, de **conserver les données de souscription de l'abonné** et **les données permettant d'identifier les utilisateurs finaux** ainsi que **les données techniques permettant d'identifier les équipements terminaux** des utilisateurs finaux ou les équipements le plus proches de ces équipements terminaux, **mais uniquement dans la mesure où ces opérateurs traitent ou génèrent ces données** dans le cadre de la fourniture de ces services ou de ces réseaux (nouvel article 126 § 1).

27. À propos du fait que le nouvel article 126 § 1er impose la collecte de certaines données, mais uniquement dans la mesure où ces opérateurs traitent ou génèrent ces données dans le cadre de la fourniture de ces services ou de ces réseaux, l'Autorité relève que les opérateurs peuvent générer et traiter (mais parfois uniquement pendant quelques secondes) des données et choisir de ne pas les enregistrer au-delà de ce traitement pour des raisons de sécurité, de respect de la vie privée ou encore de coûts. **L'Autorité rappelle qu'imposer la conservation de telles données que les opérateurs auraient choisi de ne pas conserver pour les raisons précitées constitue une ingérence particulièrement importante dans la vie privée** de toutes les personnes qui utilisent des services de communications électroniques. En effet, d'une part, il n'y a **pas de garantie que cette ingérence dans la vie privée soit effective** pour atteindre l'objectif poursuivi puisqu'il y aura toujours des possibilités **de trouver des moyens de communications qui échapperont à la surveillance étatique**. D'autre part, l'Autorité constate que **la conservation de telles données génère un risque important,** non seulement en termes de respect de la **vie privée**, mais également en termes de **sécurité de l'information** ; ce qui peut avoir un **impact financier significatif** pour les opérateurs qui sont dès lors tenus de prendre des mesures de sécurisation supplémentaires. Ce coût supplémentaire risque, *in fine*, d'être pris en charge par les consommateurs et consommatrices à la suite d'une augmentation des prix des services de communications électroniques. Ce coût supplémentaire risque également d'aboutir à ce que des services de communications électroniques

notamment, pour la jurisprudence de la CJUE, CJUE, 18 juin 2020, C-78/18, aff. « Commission c. Hongrie » et, pour la jurisprudence de la CEDH, CEDH (G.C.), 12 février 2008, App. n° 14277/04, Aff. « Guja c. Moldavie ».

gratuits et sans but de lucre[10], comme Signal ou Tor[11], ne soient plus en mesure d'offrir leurs services aux utilisateurs et utilisatrices en Belgique. **Afin d'éviter une ingérence disproportionnée** dans les droits et libertés des personnes concernées et de minimiser les risques de violation de données, l'Autorité estime que les opérateurs ne devraient être tenus de conserver, pour les besoins des autorités, les données de souscription de l'abonné et les données permettant d'identifier les utilisateurs finaux ainsi que les données techniques permettant d'identifier les équipements terminaux des utilisateurs finaux ou les équipements le plus proches de ces équipements terminaux, **uniquement dans la mesure où ils génèrent et conservent ces données pour leurs propres besoins, et pour autant, bien entendu, que cette conservation respecte les principes de nécessité et de proportionnalité**.

28. Alors que le projet de loi de réparation prévoyait une délégation au Roi pour déterminer les données qui doivent être conservées par les opérateurs en exécution de l'article 126 de la télécom, **l'amendement prévoit de lister, dans la loi télécom elle-même, les catégories de données qui doivent être conservées** par les opérateurs en exécution de cette disposition, et ce afin de **rencontrer les exigences du principe de légalité**, tel qu'il a été interprété par la Cour constitutionnelle dans son arrêt n° 158/2021. Comme le Gouvernement l'explique dans la justification de l'amendement, « *pour tenir compte de cet arrêt, les données qui se trouvaient auparavant aux paragraphes 1er des articles 3 à 6 de l'arrêté royal du 19 septembre 2013 portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques ont été déplacées vers cet article 126* ». Ainsi, **la plupart des données listées dans l'amendement sont directement reprises des articles 3 à 6 de l'arrêté du 19 septembre 2013**, tel qu'il aurait dû être modifié par le projet d'arrêté royal qui avait été soumis pour avis à l'Autorité et sur lequel elle s'est prononcée dans son avis n° 108/2021. Pour ces données, l'**Autorité renvoie donc aux considérants n° 92 à 102 de son avis n° 108/2021 pour l'examen du principe de minimisation des données**[12]**.**

[10] Ces services ne sont pas payants pour leurs utilisateurs et ils ne génèrent pas de profit à partir de la publicité.

[11] L'Autorité relève, en outre, que si ces services (qui sont utilisés certes par des personnes qui commettent des infractions, mais également par des journalistes, des lanceurs d'alerte, des militants politiques, des personnes qui défendent les droits et libertés…) étaient obligés de conserver les adresses IP qui se connectent à leurs services, non seulement cela augmenterait considérablement leur coût de fonctionnement, mais cela représenterait également un risque significatif en terme de vie privée en cas, par exemple, d'attaque par un service de renseignements étrangers (sans que les autorités belges démontrent l'utilité d'une telle conservation de données).

[12] L'Autorité souhaite toutefois continuer le dialogue que le rédacteur de l'amendement a entamé à propos des données permettant d'identifier techniquement les équipements terminaux des utilisateurs finaux (à savoir les données de type IMEI, PEI ou encore adresses MAC). En effet, dans la justification de l'amendement, l'auteur de l'amendement indique ne pas pouvoir suivre le raisonnement de l'Autorité à propos de ces données. L'auteur de l'amendement écrit « *contrairement à ce que cette Autorité indique dans son avis, une telle donnée [ndlr : les numéros d'identification des terminaux des utilisateurs finaux] à elle seule ne permet pas de 'tracer' un terminal à travers l'ensemble des services de communications électroniques qu'il utilise* ». **L'Autorité n'a jamais affirmé que ces données permettaient, <u>à elles seules</u>, de tracer un terminal à travers l'ensemble des services de communications utilisées**. Au considérant 102 de son avis n° 108/2021, l'Autorité a relevé que « Les numéros d'identification des terminaux des utilisateurs finaux constituent un identifiant unique des équipements terminaux qui permettent de 'tracer' un terminal à travers l'ensemble des services de communications électroniques qu'il utilise » et c'est, en raison de ce constat, que l'Autorité estime que l'obligation de conservation de telles données techniques permettant d'identifier les équipements terminaux des utilisateurs finaux doit être soumise aux mêmes règles que celles établies par la CJUE pour la conservation des adresses IP attribuées à la source d'une connexion. Les numéros d'identification des terminaux des utilisateurs finaux permettent, s'ils sont combinés à d'autres données, de tracer ces terminaux à travers l'ensemble des services de communications utilisés. La situation est semblable pour les adresses IP attribuées à la source de la connexion : ces

29. Outre les données déjà listées dans l'arrêté royal du 19 septembre 2013, l'**amendement prévoit d'imposer la conservation de quelques données supplémentaires** (mais toujours uniquement dans la mesure où l'opérateur traite ou génère ces données dans le cadre de la fourniture du service), à savoir :

    - **l'alias éventuel** choisi par l'utilisateur final lors de la souscription au service ou de l'activation du service, c'est-à-dire le nom par lequel l'utilisateur final se fait connaître auprès des autres utilisateurs finaux). Dans la justification de l'amendement, son auteur indique que *« Si l'utilisateur final a la possibilité de modifier son alias lors l'activation du service, l'opérateur devra conserver tant l'alias lors de la souscription que celui lors de l'activation* » ;

    - **l'adresse email de l'abonné** (comme une coordonnée de celui-ci) ;

    - **l'adresse de messagerie principale** et les **adresses de messagerie employées comme alias**.

30. L'auteur de l'amendement justifie la nécessité de conserver ces données comme suit : *« L'utilisation fréquente de fausses données d'identité impose de pouvoir recouper les données d'identification conservées avec d'autres données disponibles chez les opérateurs »,* parmi lesquelles les alias et l'adresse email de l'abonné. D'après l'auteur de l'amendement, « *ces données supplémentaires permettent d'exclure que les victimes d'une fraude à l'identité soient impliquées à tort en tant qu'auteur dans un dossier judiciaire qui ne les concerne en rien. Les données supplémentaires évitent également la violation ultérieure de la vie privée de ces personnes innocentes par des mesures d'enquête subséquentes plus intrusives, telles que l'interception de leurs communications ou une perquisition* ». **L'Autorité en prend acte**.

31. Le **nouvel article 126 § 2** de la loi télécom, introduit par l'amendement n° 1, **définit les durées de conservation des données** qui doivent être conservées en exécution de l'article 126 § 1. **Pour toutes les données**, à l'exception des adresses IP attribuées à la source d'une connexion et des identifiants uniques de l'équipement terminal de l'utilisateur, **la durée de conservation est de 12**

données ne permettent pas, à elles seules, d'effectuer le traçage exhaustif du parcours de navigation d'un internaute et, par suite, de son activité en ligne. Mais si elles sont combinées à d'autres données, les adresses IP attribuées à la source d'une connexion peuvent révéler le parcours d'un internaute sur Internet. Le parallèle que l'Autorité fait, dans son avis n° 108/2021, entre les numéros d'identification des équipements terminaux et les adresses IP attribuées à la source de la connexion apparait dès lors bien pertinent. D'ailleurs, lors d'un échange d'informations avec le délégué du Ministre dans le cadre de la mise en état du dossier ayant abouti à l'avis n° 108/2021, celui-ci a d'ailleurs reconnu que le raisonnement suivi pour la CJUE à propos des adresses IP pouvait être suivi quant aux autres données techniques nécessaires pour identifier utilisateur final, l'équipement terminal, le service de communication électroniques employé. **Il s'ensuit que, comme l'Autorité l'a déjà souligné dans son avis n° 108/2021, la conservation de ces données ne devrait être imposée qu'afin de poursuivre un objectif présentant une importance particulière (comme la lutte contre la criminalité grave), la durée de leur conservation devrait être strictement limitée au regard de cet objectif et il faudrait prévoir des conditions et des garanties strictes quant à l'exploitation de ces données** (voyez CJUE, arrêt du 6 octobre 2020, § 156)**.**

mois après la fin du service. Pour les **adresses IP attribuées à la source d'une connexion** et les **identifiants uniques de l'équipement terminal de l'utilisateur** (à savoir : l'identité internationale d'équipement mobile ("IMEI"), l'identifiant permanent de l'équipement ("PEI"), l'adresse du contrôleur d'accès au réseau ("MAC")), la durée de conservation est de **12 mois après la fin de la session**. Pour les **adresses MAC**, la durée de conservation est de **6 mois après la fin de la session**[13], si l'opérateur conserve une autre donnée d'identification de l'équipement terminal de l'utilisateur. **L'Autorité prend note de ces durées de conservation**.

C. Concernant les amendements n° 2 et 3

32. L'amendement n° 2 entend remplacer le paragraphe 2 de l'article 126/1 de la loi télécom, tel qu'il sera modifié par le projet de loi de réparation. Pour rappel, le nouvel article 126/1 de la loi télécom, tel qu'il sera modifié par le projet de loi de réparation, **impose** aux opérateurs de conserver, en principe, **pendant 12 mois**[14], les **données de trafic et de localisation** de **toutes les communications** effectuées **à partir**, ou **vers**, une des **zones géographiques** qu'il liste. Ces données ne devront être conservées que si les opérateurs les génèrent ou les traitent déjà dans le cadre de la fourniture des services de communications électroniques qu'ils offrent ou des réseaux de communications électroniques qu'ils mettent à disposition[15]. Cette conservation est imposée « *aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave, de la prévention de menaces graves contre la sécurité publique, et de la sauvegarde des intérêts vitaux d'une personne physique* ». Ainsi, le nouvel article 126/1 de la loi télécom entend imposer, en vue de poursuivre des objectifs présentant une importance particulière, à l'instar de la lutte contre la criminalité grave, une **conservation préventive des données de trafic et de localisation qui soit ciblée en fonction de critères géographiques.** L'Autorité renvoie aux **considérants n° 106 à 130 de son avis n° 108/2021** dans lequel elle a examiné la conformité de cette disposition avec les exigences issues du droit à la protection des données, tel qu'il est consacré, en particulier, par la Charte des droits fondamentaux de l'Union européenne et la Directive ePrivacy. **L'Autorité relève qu'elle a, notamment, émis des craintes fondamentales à propos de cette disposition**, en particulier quant au fait que les critères retenus par le projet de loi de réparation pour déterminer les zones géographiques dans lesquelles une obligation de conservation des données de trafic est imposée de manière préventive pourraient aboutir à réintroduire, *de facto*, une obligation de conservation quasi-généralisée et

[13] À propos de la conservation des adresses MAC, l'Autorité relève que les adresses MAC sont modifiées très régulièrement (depuis 2014). La collecte de cette information nécessite dès lors un stockage massif de données et n'est que peu utile. Voyez, par exemple, https://en.wikipedia.org/wiki/MAC_address#Randomization: "MAC address randomization during scanning was added in Android starting from version 6.0,[19] Windows 10,[21] and Linux kernel 3.18.[22].

[14] A moins qu'une autre durée soit prévue par ce nouvel article 126/1 de la loi télécom. Cette disposition prévoit des durées de conservation plus courtes dans certaines circonstances. Voyez le nouvel article 126/1 § 3, 1° de la loi télécom.

[15] Il est précisé, dans l'Exposé des motifs, que « *les données ne sont conservées par les opérateurs concernés que dans la mesure où ces données ont été générées ou traitées par eux dans le cadre de la fourniture des services de communication concernés, et uniquement dans les zones géographiques prédéfinies. En d'autres termes, il n'y a aucune obligation de conserver les données lorsque celles-ci :*
1° ne sont pas générées ou traitées par les opérateurs concernés,
2° ne sont pas générées ou traitées dans les zones géographiques déterminées au paragraphe 3 ».

indifférenciée des données de trafic. En outre, l'Autorité souligne que certains opérateurs de services de communications électroniques, à l'instar de Signal, n'ont pas accès aux données de localisation de leurs abonnés. Aux termes du nouvel article 126/1 de la loi télécom, ces services devraient dès lors collecter, de manière préventive, les données de trafic de tous leurs abonnés ; ce qui irait à l'encontre du principe de proportionnalité, tel qu'il a été interprété par la CJUE[16].

33. Dans le projet de loi de réparation, il était prévu de déléguer au Roi le pouvoir de déterminer les données qui devaient être conservées en exécution de cette disposition. **Le Gouvernement a décidé, à la suite de l'arrêt n° 158/2021, d'énumérer, dans la loi elle-même, les métadonnées qui doivent être conservées en exécution de cette disposition**. Ainsi, l'article 126/1 § 2, tel qu'il est remplacé par l'amendement n° 2, prévoit que « *les métadonnées de communications électroniques, en ce compris les métadonnées pour les appels infructueux, auxquelles s'applique l'obligation de conservation visée au paragraphe 1er sont énumérées à l'article 126/2* ». L'amendement n° 3, qui entend insérer l'article 126/2 dans la loi télécom, liste les données qui doivent être conservées en exécution de l'article 126/1. Comme c'est le cas pour les données qui doivent être conservées en exécution de l'article 126, **la plupart des données listées dans l'amendement n° 3 sont directement reprises des articles 3 à 6 de l'arrêté du 19 septembre 2013**, tel qu'il aurait dû être modifié par le projet d'arrêté royal qui avait été soumis pour avis à l'Autorité et sur lequel elle s'est prononcée dans son avis n° 108/2021. L'Autorité renvoie dès lors à son avis n° 108/2021 pour l'analyse de ces données[17].

34. **Plusieurs nouveautés** toutefois :

- la conservation de « *l'alias éventuel choisi par l'utilisateur final lors de la souscription au service ou de l'activation du service* » (2°)

- l'identifiant unique pour les appels individuels (« SIP call ID ») (4°)[18]

[16] Voyez, notamment, CJUE, arrêt du 6 octobre 2020, § 141 et suivants. L'Autorité renvoie, en outre, aux considérants n° 129 et 130 de son avis 108/2021 dans lequel elle relève que la disposition qui prévoit que « *Lorsque la technologie utilisée par l'opérateur ne permet pas de limiter la conservation de données aux zones visées au paragraphe 3, il conserve au moins les données nécessaires pour couvrir l'entièreté de la zone concernée tout en limitant la conservation de données en dehors de cette zone au strict nécessaire au regard de ses possibilités techniques* » n'est pas admissible.

[17] Elle constate d'ailleurs que le rédacteur de l'amendement a pris en compte sa remarque selon laquelle « la conservation des données de trafic ne doit pas contenir ou permettre de déduire l'url spécifique des pages web visitées par les personnes concernées ». En effet, l'amendement n° 3 indique que « *pour les services de communications électroniques à l'exception des services d'accès à Internet, l'adresse IP utilisée par le destinataire de la communication, l'horodatage ainsi que, en cas d'utilisation partagée d'une adresse IP du destinataire, les ports qui lui ont été attribués* » (c'est l'Autorité qui souligne). Pour les services d'accès à Internet, l'adresse IP du destinataire (qui permettrait d'identifier l'url de la page web visité) ne doit pas être conservée.

[18] La conservation de cette donnée est justifiée comme suit : « *Le « SIP call ID » permet d'identifier chaque appel individuel en Voice-over-IP de façon fiable. Le « SIP call ID » est une donnée importante à conserver puisqu'à l'avenir la majeure partie des appels téléphoniques est amenée à devenir du trafic SIP* ».

- les données permettant d'identifier et de localiser les cellules ou d'autres points de terminaison du réseau, qui ont été utilisé(e)s pour effectuer la communication, du début jusqu'à la fin de la communication, ainsi que les dates et heures précises de ces différentes localisations (alors que dans la version antérieure, seule la localisation des cellules ou d'autres points de terminaison du réseau utilisée au début et à la fin de la communication devait être conservée)[19] (7°)

- pour ce qui concerne les services de communications électroniques mobiles, la date et l'heure de la connexion de l'équipement terminal au réseau en raison du démarrage de cet équipement et le moment de la déconnexion de cet équipement au réseau en raison de l'extinction de cet équipement (9°)[20]

- pour ce qui concerne les services de communications électroniques mobiles, la localisation de l'équipement terminal et la date et l'heure de cette localisation chaque fois que l'opérateur cherche à connaître la présence des équipements terminaux sur son réseau (10°)[21]

- la conservation de « *toute donnée ayant une fonction équivalente [mais à quoi ?]* » lorsqu'une donnée précitée n'est pas disponible (11°)

35. Tout d'abord, l'Autorité constate que **la justification de l'amendement ne démontre pas pourquoi il est nécessaire pour atteindre la finalité poursuivie par la conservation de ces données**, à savoir la lutte contre la criminalité grave, **de conserver la date et l'heure de la connexion** de l'équipement terminal au réseau en raison du démarrage de cet équipement **et le moment de la déconnexion** de cet équipement au réseau en raison de l'extinction de cet équipement (9°) et **la localisation de l'équipement terminal** et la date et l'heure de cette

[19] La justification de l'amendement indique ce qui suit : « *Une nouvelle exigence est ajoutée par rapport l'arrêté royal de 2013 : les opérateurs doivent désormais conserver la localisation des cellules et autres points de terminaison du réseau tout au long de la communication (par exemple, les mâts intermédiaires, ou les routeurs Wifi dans le cadre de services nomades) et pas uniquement leur localisation au début et à la fin de la communication. Une telle exigence prend tout son sens lorsque l'utilisateur final se déplace. Une telle information est capitale pour les services de sécurité. Les données de localisation que les opérateurs doivent conserver en dehors de toute communication sont prévues au paragraphe 2, 10°. L'article 5, § 2, 3° de l'AR de 2013 ne mentionnait l'identification et la localisation du point de terminaison du réseau utilisé par l'utilisateur final qu'au début et à la fin d'une connexion. Dans le cadre de la technologie 2G et 3G, ceci permettait effectivement de localiser la communication réalisée au départ de cette technologie. Ce type d'utilisation est devenu obsolète depuis la généralisation des smartphones avec connexion de données permanente puisqu'avec cette technologie, une session data peut durer de nombreuses heures (parfois supérieure à 12 heures). Cela a pour conséquence qu'un utilisateur pourrait erronément être localisé à un endroit alors qu'il ne s'y trouve plus depuis de nombreuses heures*. Cette localisation erronée risque d'emporter des conséquences, à charge ou à décharge, des citoyens. ».

[20] La justification de l'amendement indique ce qui suit : « *Alors que les articles 4, § 2, 6° et 5, § 2, 3° de l'arrêté royal de 2013 contenaient une obligation large pour les opérateurs en matière de conservation de données de connexion, le nouveau paragraphe 2, 9° de l'article 126/2 en projet prévoit la conservation de certaines données de connexion indépendantes d'une communication, à savoir les données de (dé)connexion qui sont générées par l'allumage ou l'extinction du téléphone mobile* ».

[21] La justification de l'amendement indique ce qui suit : « *De même, le nouveau paragraphe 2, 10° de l'article 126/2 en projet prévoit la conservation de la localisation de l'équipement terminal en dehors de toute communication, dans le cadre des opérations que fait l'opérateur régulièrement pour connaitre la présence des équipements terminaux sur son réseau. Ceci est techniquement nécessaire pour en conserver la performance, pour maintenir un niveau de service élevé, assurer le transit rapide des appels et des communications qu'ils doivent traiter, etc. Pour ce faire, diverses méthodes sont utilisées. Il peut par exemple s'agir de « LBS » (« Localisation Base Services ») ou de « paging ». La fréquence et la méthode de ces opérations est variable. Elle dépend des nécessités techniques propres au réseau de l'opérateur, telles que le type de technologie utilisée (2G, 3G, 4G, etc.) ou la densité d'utilisateurs présents sur une partie du réseau* ».

localisation chaque fois que l'opérateur cherche à connaître la présence des équipements terminaux sur son réseau (10°). **Soit l'auteur de l'amendement est en mesure de montrer en quoi la conservation de ces catégories de données est nécessaire et proportionnée au regard de l'objectif poursuivi, et cette explication est ajoutée dans la justification de l'amendement, soit l'ajout de ces nouvelles catégories de données (ou du moins celles pour lesquelles l'auteur n'est en mesure d'en justifier la conservation) doit être supprimée**.

36. Ensuite, à propos la donnée listée au 11° de l'article 126/2 § 2 (*« lorsqu'une donnée précitée n'est pas disponible, toute donnée ayant une fonction équivalente* »), l'Autorité relève que **sa définition n'est pas suffisamment prévisible** pour permettre aux personnes concernées d'identifier la donnée qui sera effectivement conservée par les opérateurs sur cette base. Or, au vu de l'ingérence particulièrement importante générée par la conservation des données de trafic et de localisation en exécution de l'article 126/1 (qui permettent d'identifier avec qui a communiqué avec qui, pendant combien de temps, et à partir de quel endroit), il est essentiel que la norme qui encadre ce traitement de données soit particulièrement précise et prévisible. **L'amendement sera modifié afin de supprimer l'article 126/2, § 2, 11°[22].**

D. Concernant l'amendement n° 6

37. L'amendement n° 6, qui entend **remplacer l'article 127 dans la loi télécom**, vise à répondre à l'annulation par la Cour constitutionnelle de l'article 2 de la loi du 1er septembre 2016 « *portant modification de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité* », uniquement en ce qu'il ne détermine pas les données d'identification qui sont collectées et traitées et les documents d'identification qui entrent en considération.

38. L'article 127 de la loi télécom entend **obliger les opérateurs à identifier leurs abonnés** pour les besoins des autorités ou à conserver des informations qui permettront aux autorités de les identifier ultérieurement[23]. À la différence de ce qui était prévu dans la version antérieure de cette disposition

[22] Si l'auteur ne suit pas la recommandation de l'Autorité de supprimer l'article 126/2 § 2, 11°, il faut à tout le moins compléter le dispositif comme suit : « lorsqu'une donnée précitée n'est pas disponible, toute donnée ayant une fonction équivalente, mais à condition qu'elle ne contienne pas plus d'information que les données précitées » ; et ce afin de respecter le principe de minimisation des données.

[23] Les autorités habilitées à recevoir l'identité des abonnés et utilisateurs finaux des services de communications électroniques sont les suivantes :
« *1° les services de renseignement et de sécurité, afin d'accomplir les missions qui leur sont attribuées par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité ;*
2° les autorités compétentes aux fins de la prévention de menaces graves pour la sécurité publique ;
3° les autorités chargées de la sauvegarde des intérêts vitaux de personnes physiques ;
4° les autorités compétentes pour l'examen d'une défaillance de la sécurité du réseau ou du service de communications électroniques ou des systèmes d'information ;
5° les autorités administratives ou judiciaires compétentes pour la prévention, la recherche, la détection ou la poursuite d'une infraction commise en ligne ou par le biais d'un réseau ou service de communications électroniques ;

(dans le projet de loi de réparation), la version de l'article 127 qui est reprise dans l'amendement n° 6 **liste les données d'identification** qui doivent être traitées et conservées par les opérateurs dans le cadre de l'obligation d'identification des abonnés et utilisateurs finaux de leurs services.

39. Comme la justification de l'amendement le précise, *« Le paragraphe 1er de l'article 127 est un paragraphe général et décrit son champ d'application (entre autres les opérateurs et services de communications électroniques auxquels il s'applique). Les paragraphes 2 à 9 sont relatifs à l'identification par un opérateur de l'abonné (la personne qui conclut le contrat avec l'opérateur). Le paragraphe 10 est consacré à l'identification de l'utilisateur effectif du service. Le paragraphe 11 est un paragraphe général et décrit les sanctions applicables lorsque les opérateurs ou les abonnés ne respectent pas les obligations qui leur incombent* ».

1. À propos de l'extension de l'obligation d'identification des abonnés et des utilisateurs finaux de services de communications électroniques

40. L'Autorité constate que **le nouvel article 127 étend considérablement l'obligation d'identification des abonnés et des utilisateurs finaux de services de communications électroniques** :

- Premièrement, à la suite de la modification des définitions des notions d'« *opérateur* » et de « *service de communications électroniques* » (*cf. supra,* cons. 23-24), **l'obligation d'identification imposée par le nouvel article 127 concernera l'utilisateur de beaucoup plus de services de communications électroniques que ce qui est prévu dans le cadre normatif actuel.** En effet, cette obligation s'imposera à tous les services de communications électroniques qui correspondent à la nouvelle définition de cette notion, laquelle inclut notamment, les services de communications interpersonnelles qui ne sont pas fondés sur la numérotation (les « OTT », comme WhatsApp, Messenger, Signal, Telegram, Tik Tok,…) et les services de communications offerts pour permettre des applications « M2M » (Internet des objets/objets connectés). En outre, il convient de souligner que l'obligation d'identification s'appliquera tant pour les services de communications électroniques fournis contre paiement que pour ceux qui sont fournis gratuitement. Par comparaison, la version actuelle de l'article 127 de la loi télécom[24] délègue au Roi le soin de déterminer les mesures techniques et administratives qui sont imposées aux opérateurs en vue de permettre l'identification de l'utilisateur final. Cette disposition a été

6° les autorités administratives ou judiciaires compétentes pour la prévention, la recherche, la détection ou la poursuite d'un fait qui relève de la criminalité grave ;
7° les autorités administratives chargées de préserver un intérêt économique ou financier important de l'Union européenne ou de la Belgique, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale ;
8° les autorités administratives ou judiciaires compétentes pour la prévention, la recherche, la détection ou la poursuite d'un fait qui constitue une infraction pénale mais qui ne relève pas de la criminalité grave » (article 127/1 § 3, alinéa 1er).

[24] C'est-à-dire celle qui a été annulée par la Cour constitutionnelle dans son arrêt n° 158/2021, mais uniquement dans la mesure où cette disposition ne détermine pas les données d'identification qui sont collectées et traitées et les documents d'identification qui entrent en considération

exécutée par l'arrêté royal du 27 novembre 2016[25] uniquement pour ce qui concerne les services de communications électroniques qui sont offerts sur la base d'une carte de téléphonie mobile prépayée. En outre, dans le contexte normatif actuel, les détenteurs d'une carte SIM utilisée uniquement dans le cadre d'une communication « M2M » ne sont pas soumis à une obligation d'identification[26].

- Deuxièmement, les **autorités qui pourront avoir accès aux données d'identification** des abonnés aux services de communications électroniques seront **plus nombreuses** que celles qui peuvent avoir accès à ces données dans la version actuelle des articles 126 et 127.

- Troisièmement, comme l'auteur de l'amendement n° 6 l'indique, « *l'ancien article 127, § 2, contenait une interdiction pour les opérateurs de rendre difficile ou impossible l'identification des utilisateurs finaux. Le* ***nouvel article 127 comprend dorénavant une obligation positive pour les opérateurs d'identifier leurs abonnés (méthode d'identification directe) ou à tout le moins de rendre cette identification possible (méthode d'identification indirecte)*** ».

- Quatrièmement, le nouvel article 127 § 1 interdit, sous peine de sanction pénale, de distribuer en Belgique des cartes prépayées ou des abonnements qui permettent aux utilisateurs finaux d'y utiliser un service de communications électroniques ou encore des objets connectés qui permettent l'utilisation d'un service d'accès à Internet ou d'un service de communication interpersonnelle, sans avoir obtenu l'accord de l'entreprise qui fournit ce service de communications électroniques accessible au public. L'entreprise qui donne son accord doit être considérée comme un opérateur tenu au respect de l'obligation imposée par ce nouvel article 127. **Cette interdiction vise à empêcher tout contournement de l'obligation qui pèse sur les opérateurs d'identifier les utilisateurs finaux des services de communications électroniques qu'ils fournissent**.

41. Cette extension de l'obligation d'identification des utilisateurs finaux des services de communications électroniques **augmente considérablement l'ingérence dans leurs droits et libertés**[27]. Certes, les objectifs poursuivis par cette extension – et plus largement par l'identification des utilisateurs de services de communications électroniques – sont légitimes. Mais la légitimité des objectifs poursuivis ne suffit pas à justifier l'ingérence dans les droits et libertés des personnes concernées. Il faut, en outre, s'assurer que cette ingérence est adéquate/pertinente, qu'elle est nécessaire et, enfin qu'elle est strictement proportionnée à l'objectif poursuivi. En d'autres termes, **la fin ne justifie pas, à elle**

[25] Voyez l'arrêté royal du 27 novembre 2016 « relatif à l'identification de l'utilisateur final de services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée » (ci-après « l'arrêté royal du 27 novembre 2016 »)
[26] Article 1er, alinéa 3, de l'arrêté royal du 27 novembre 2016.

[27] L'Autorité rappelle, à ce propos, que la CJUE avait, dans son arrêt « Quadrature du Net », relevé que « ***les internautes disposent,*** *conformément à ce qui a été constaté au point 109 du présent arrêt,* ***du droit de s'attendre,*** *en vertu des articles 7 et 8 de la Charte,* ***à ce que leur identité ne soit, en principe, pas dévoilée*** » (§ 155).

seule, les moyens. C'est pourquoi l'Autorité invite les parlementaires à **analyser en profondeur la pertinence, la nécessité et la proportionnalité d'une telle extension de l'obligation d'identification des utilisateurs finaux des services de communications électroniques, en prenant en compte, notamment, les implications de cette extension sur l'exercice du droit à la vie privée et du droit à la liberté d'expression**. Lors de cette analyse, l'Autorité invite les parlementaires à prendre également en compte le fait que les criminels qui souhaitent échapper à la surveillance des moyens de communications électroniques par les autorités trouveront d'autres moyens de communication qui leur permettront de préserver leur anonymat. C'est pourquoi **l'Autorité invite les parlementaires à être particulièrement attentifs à ne pas réduire les libertés de la quasi-entièreté de la population par l'adoption d'une mesure** (obligation d'identification des utilisateurs de tous les moyens de communications électroniques) **s'il s'avérait que celle-ci n'était, en fait, pas pertinente et nécessaire, notamment parce qu'il apparaitrait que les « criminels » pourraient raisonnablement trouver d'autres moyens de communication en vue d'échapper à la « surveillance » des services de communications électroniques par les autorités**.

2. À propos de la qualité de l'identification de l'abonné

42. Par ailleurs, l'Autorité estime également essentiel d'attirer l'attention des parlementaires sur le fait que **l'identification de l'abonné à un service de communications électroniques ne permet pas nécessairement d'identifier l'utilisateur effectif de ce service**. Certes, le nouvel article 127 § 10 de la loi télécom entend créer une présomption selon laquelle « *Sauf preuve contraire, la personne identifiée est présumée utiliser elle-même le service de communications électroniques* » (*cf. infra*, cons. 78). Toutefois, dans les faits, il n'est pas rare que l'utilisateur d'un service de communications électroniques soit différent de la personne ayant souscrit à ce service. Il existe donc un **risque réel** que l'utilisateur final ne soit **pas identifié de manière certaine** et que la **qualité des données d'identification** de l'utilisateur final **puisse être remise en cause**. Les incertitudes quant à la qualité des données d'identification seront **d'autant plus importantes** que l'identification de l'abonné aura lieu par le biais **d'une méthode d'identification indirecte**. En effet, l'identification de la personne « derrière » une adresses IP, un numéro de téléphone ou la référence d'une transaction bancaire ne permet pas d'identifier de manière certaine la personne qui a effectivement utilisé le service de communications électroniques. **Dans ces circonstances où la qualité de l'identification de l'utilisateur effectif** du service de communications électroniques **apparait incertaine**, l'Autorité insiste pour que les parlementaires réfléchissent sur, et justifient, **la nécessité de l'ingérence** causée dans le droit à la protection des données à caractère personnel des abonnés de services de communications électroniques.

43. L'amendement n° 6 **distingue les modalités** de l'obligation d'identification des abonnés **selon le caractère gratuit ou payant** du service de communications électroniques. S'il s'agit d'un **service payant**[28], le nouvel article 127 de la loi télécom impose, en principe, aux opérateurs d'identifier leurs abonnés au moyen d'une **méthode d'identification directe**[29] ou « *en collectant et conservant la référence de l'opération de paiement, le nom, le prénom, le lieu et la date de naissance de l'abonné* » (qui est une méthode d'identification indirecte) (sur le fait qu'aux termes du principe de minimisation des données, le « *lieu et la date de naissance* » ne peuvent pas être conservés, voyez cons. 75). Le nouvel article 127 prévoit toutefois que, pour certains services de communications électroniques payants, l'identification pourra avoir lieu selon d'autres modalités qu'il précise. Lorsque le service de communications électroniques est **gratuit**, l'opérateur doit identifier ses abonnés à l'aide d'une des **méthode d'identification indirecte**[30] visée au paragraphe 9 de cette disposition[31], à savoir, notamment, la conservation de l'adresse IP ayant servi à la création du compte qui permet l'utilisation du service de communications électroniques et des adresses IP à la source de la connexion, l'horodatage ainsi que, en cas d'utilisation partagée d'une adresse IP de l'utilisateur final, des ports qui lui ont été attribués ou la collecte et la conservation du numéro de téléphone de l'abonné attribué dans le cadre d'un service de communications électroniques payant pour lequel un opérateur doit identifier l'abonné (voyez, *infra*, les cons. 72 et suivants pour les observations à ce propos).

[28] Le nouvel article 127 définit le service de communications électroniques payant comme « *le service de communications électroniques pour lequel un paiement de l'abonné à l'opérateur est nécessaire pour utiliser le service ou continuer à l'utiliser, ainsi que tout service de communications électroniques offert sans surcoût par l'opérateur à l'abonné conjointement à ce service* ».

[29] Le nouvel article 127 définit la méthode d'identification directe comme suit : « *méthode par laquelle l'opérateur collecte et conserve des données fiables relatives à l'identité civile d'une personne physique qui est son abonné ou qui agit pour le compte de son abonné qui est une personne morale afin de remplir les obligations d'identification de la personne morale et, le cas échéant, une copie du document d'identification de cette personne physique* ».

[30] Le nouvel article 127 définit la méthode d'identification indirecte comme suit : « *méthode par laquelle l'opérateur collecte et conserve des données qui permettent aux autorités visées à l'article 127/1, § 3, alinéa 1er, d'obtenir d'un tiers l'identité de ses abonnés* ».

[31] Le choix du législateur d'imposer l'identification par le biais d'une méthode indirecte, plutôt que par une méthode d'identification directe, repose sur des considérations liées au respect de la vie privée des utilisateurs. En effet, selon la justification de l'amendement, « *Les opérateurs qui offrent des services gratuits sont généralement des opérateurs qui offrent des services de communications interpersonnelles qui ne sont pas basés sur la numérotation (les « OTT »). Ils ne disposent généralement pas des données d'identité civile de leurs abonnés (ou en tous cas pas de données dont la fiabilité a été vérifiée) ni de copie de leurs documents d'identité, vu que cela n'est pas nécessaire pour qu'ils offrent leurs services. Le chiffre d'affaires effectué par ce type d'opérateur provient généralement du traitement des données de l'abonné et de l'envoi de publicités à ce dernier. Le gouvernement souhaite éviter que les opérateurs dont le modèle commercial est basé sur le traitement des données de l'abonné mettent en place une méthode d'identification directe, étant donné que cela impliquerait qu'ils pourraient relier les (parfois nombreuses) données qu'il détienne déjà sur l'abonné avec l'identité de ce dernier, ce qui rendrait le traitement de ses données plus sensible. L'identification indirecte est plus appropriée pour les services gratuits, étant donné que cette méthode d'identification présente l'avantage que l'opérateur ne connaît pas lui-même l'identité de son abonné lorsqu'il n'est pas nécessaire qu'il la connaisse* » (c'est l'Autorité qui souligne). L'Autorité prend acte de la volonté de l'auteur de l'amendement de combiner l'objectif poursuivi par l'identification des abonnées pour le besoin des autorités avec le principe de minimisation des données. Elle note toutefois que certains opérateurs offrent un service de communications électroniques, comme Signal ou Tor, sans collecter des données de ses abonnés et n'ont pas de but de lucre (ils ne gagnent pas d'argent en envoyant des publicités à leurs abonnés).

3. *À propos de (l'absence de) conservation des données et documents d'identification par les points de vente* (article 127 § 3, alinéas 1er et 2)

44. Le nouvel article 127 § 3, alinéas 1er et 2, prévoit que « *Le point de vente de services de communications électroniques ne conserve pas de données d'identification ni de copie de documents d'identité, qui sont transmis à l'opérateur ou à l'entreprise fournissant un service d'identification. Si une introduction directe dans les systèmes informatiques de l'opérateur ou de l'entreprise fournissant un service d'identification n'est pas possible, le point de vente de services de communications électroniques peut faire une copie du document d'identification, dont la carte d'identité électronique belge, mais cette copie est détruite au plus tard après l'activation du service de communications électroniques* ».

45. L'Autorité **prend note de la garantie** selon laquelle le point de vente de services de communications électroniques ne conserve pas de données d'identification ni de copie de documents d'identité**.**

46. Toutefois, l'Autorité rappelle que la **copie de documents d'identité génère des risques importants pour les droits et libertés des personnes concernées** (en particulier des risques de fraude à l'identité). Il convient dès lors de limiter, au maximum, la prise de copie de documents d'identité aux seuls cas où cela s'avère strictement nécessaire. En l'espèce, l'Autorité souligne qu'il serait préférable de prévoir une obligation, pour les points de vente, d'introduire les données d'identification directement dans les bases de données qui doivent être tenues par les opérateurs en exécution de l'article 127[32]. **Le nouvel article 127 § 3, alinéas 1er et 2, sera modifié afin d'imposer aux points de vente de services de communications électroniques l'introduction des données d'identification de l'abonné directement dans les systèmes informatiques de l'opérateur ou de l'entreprise fournissant un service d'identification et leur interdire toute prise de copie de document d'identité.**

4. *À propos de la durée de conservation des données et documents d'identification (article 127 § 3, dernier alinéa)*

47. Le nouvel article 127 § 3, dernier alinéa, détermine la **durée de conservation** des données d'identification et éventuelles copies des documents d'identification collectées en vertu de l'article 127 : **12 mois après la fin du service de communications électroniques**. L'Autorité **en prend note**.

[32] S'il n'est pas possible d'imposer une telle obligation pour les points de vente (ce qu'il conviendra de justifier, dans le respect des principes de nécessité et de proportionnalité, à l'aide d'éléments factuels et concrets), il convient, au moins, d'entourer la prise de copie des documents d'identité de garanties. À ce propos, conformément à la recommandation 03/2011 de la Commission de la protection de la vie privée (ci-après « la CPVP »), l'Autorité recommande au législateur d'indiquer que la copie de la carte d'identité devrait être barrée et qu'il devrait y être fait mention de son destinataire et de l'usage que peut en faire son destinataire. Comme l'avait soulevé la CPVP à l'époque, ce procédé permet d'éviter toute reproduction conforme de la carte d'identité et de limiter toute utilisation pour des finalités détournées. CPVP, Recommandation n° 03/2011 du 25 mai 2011 relative à la prise de copie de carte d'identité ainsi qu'à leur utilisation et à leur lecture électronique, p. 21.

5. À propos de l'obligation de s'assurer la fiabilité de l'identification (article 127 § 4, alinéas 1 et 2)

48. Le nouvel article 127 § 4, alinéas 1er et 2, de la loi télécom impose à l'opérateur de « *[mettre] tout en œuvre pour s'assurer de la* ***fiabilité de l'identification*** *de l'abonné qui est une personne physique. Il s'assure que les données d'identification collectées correspondent aux données sur le document d'identité. Il vérifie* :
    - *que le document d'identification que l'abonné soumet pour s'identifier est l'original, lisible et présente l'apparence d'authenticité*
    - *que la date de validité de ce document n'est pas dépassée*
    - *que ce document est relatif à la personne identifiée* ».

5.1. Sur l'autorisation de recourir à la reconnaissance faciale pour s'assurer la fiabilité de l'identification (article 127 § 4, alinéa 3)

49. Afin d'assurer cette fiabilité, l'article 127 § 4, alinéa 3, permet à l'opérateur ou au point de vente du service de communications électronique de réaliser « *de manière automatique, une comparaison entre les paramètres biométriques sur la photo du document d'identité de l'abonné et ceux de son visage* ».

50. Le projet **d'amendement prévoit** certaines **garanties** pour les droits et libertés des personnes concernées :
    - Le Ministre des télécommunications et le Ministre de la justice doivent avoir autorisé l'opérateur ou l'entreprise qui propose la méthode de comparaison entre les paramètres biométriques sur la photo du document d'identité de l'abonné et ceux de son visage à recourir à cette méthode, étant donné que cette autorisation « *a pour objectif de vérifier la fiabilité de cette comparaison pour les besoins des autorités* »[33] (nouvel article 127 § 4, alinéas 3 à 5).

[33] À ce propos, la justification de l'amendement précise que « *L'autorisation ministérielle prévue pour valider cette méthode d'identification au cas par cas ne porte que sur la question de savoir si cette méthode est suffisamment fiable pour les services de sécurité (en particulier la police et les services de renseignement et de sécurité). Cette autorisation n'a pas pour objet de se prononcer sur le respect de la législation visant à protéger la vie privée des abonnés* ». L'Autorité en prend note, mais elle indique que **la question de savoir si une méthode de reconnaissance faciale est « suffisamment fiable » relève bien du respect de la législation visant à protéger la vie privée des abonnés** puisque l'article 5.1.c) et 5.1.d) du RGPD impose que les données traitées soient adéquates et pertinentes au regard des finalités pour lesquelles elles sont traitées et qu'elles soient exactes. Par ailleurs, l'Autorité relève que si la comparaison automatisée entre les paramètres biométriques sur la photo du document d'identité d'une personne et ceux de son visage peut actuellement être très fiable, **les systèmes de reconnaissance faciale se sont révélés vulnérables aux attaques de « morphing »**. Dans ces attaques, les images faciales de deux individus (ou plus) sont combinées (morphées) et l'image faciale morphée résultante est ensuite présentée lors de l'enregistrement comme une référence biométrique. Si l'image morphée est acceptée, il est probable que tous les individus ayant contribué à l'image faciale morphée puissent être identifiés avec succès par rapport à celle-ci. Les attaques par morphing constituent donc une menace sérieuse pour les systèmes de reconnaissance faciale**. Cette vulnérabilité crée un risque de fraudes à l'identité**. La mesure la plus efficace pour contrer ce type d'attaque serait que la photo qui figure sur les documents d'identité soit prise directement par l'autorité qui délivre ledit document d'identité. Il ne semble pas que cela soit prévu dans un futur à court ou à moyen terme (voyez, à ce sujet, J. Merkle, C. Rathgeb, U. Scherhag, C. Busch, R. Breithaupt: "Face Morphing Detection: Issues and Challenges", in Proceedings International Conference on Biometrics for Borders (ICBB), Frontex, Warsaw, October 9-10, (2019)).

- L'abonné doit donner son consentement, étant donné que l'article 127 § 4, alinéa 6, impose à l'opérateur d'offrir au moins une manière alternative de s'identifier.
- *« L'opérateur et le point de vente ne peuvent communiquer ces paramètres biométriques à un tiers au sens de l'article 4, 10) du RGPD. Ils ne peuvent les traiter que dans les limites nécessaires en vue d'accomplir la finalité de comparaison faciale visée à l'alinéa 3 [à savoir : assurer la fiabilité de l'identification de l'abonné]* ».

51. Le projet de loi de réparation prévoyait déjà de permettre à l'opérateur ou au canal de vente de services de communications électroniques de recourir à une méthode de reconnaissance faciale (qui vise à comparer, de manière automatique, les paramètres biométriques sur la photo de la pièce d'identité de l'abonné et ceux de son visage). Au considérant 104 de son avis n° 108/2021, l'Autorité indiquait que « Le recours à des techniques de reconnaissance faciale pour identifier les abonnés excède ce qui est nécessaire dans une société démocratique alors qu'il existe, en Belgique, d'autres moyens plus surs et moins intrusifs (l'utilisation de l'eID ou d'Itsme) pour authentifier électroniquement des personnes ». Dans la justification de l'amendement, le Gouvernement indique ne pas pouvoir suivre l'avis de l'Autorité concernant le caractère particulièrement intrusif du recours à la reconnaissance faciale dans le contexte de l'identification des abonnés aux services de communications électroniques. Le gouvernement indique, dans la justification de l'amendement, qu'il « *est d'avis que la comparaison faciale qui est mise en œuvre pour l'identification de l'utilisateur final ne constitue pas une intrusion dans la vie privée des abonnés. En effet, les données biométriques ne seront en pratique pas conservées. Le gouvernement est d'avis que le traitement de données biométriques prévu par l'article 127 est moins sensible d'un point de vue vie privée que la reconnaissance faciale ou des empreintes digitales qui permettent de déverrouiller un smartphone, étant donné que dans le deuxième cas de figure, les données biométriques doivent être conservées. Il n'est pas admissible que la législation soit plus stricte pour une finalité publique (identification de l'abonné dans le cadre de l'article 127) que pour des usages du secteur privé (ex. déverrouiller un smartphone)* ».

52. Tout d'abord, l'Autorité rappelle que, contrairement à ce qu'avance le Gouvernement, le traitement de données à caractère personnel – en particulier **la comparaison automatisée entre les paramètres biométriques sur la photo du document d'identité de l'abonné et ceux de son visage** – constitue, bien évidemment, **une ingérence dans la vie privée des abonnés**, quand bien même les données biométriques ne sont pas conservées. Cette ingérence présente d'ailleurs un caractère particulièrement important au vu du caractère sensible des données traitées et des risques de fraude à l'identité qui découlent d'une violation de telles données[34]. En effet, l'utilisation de la technologie de

[34] Les paramètres biométriques sur la photo du document d'identité de l'abonné constituent, en effet, des données qui relèvent de l'article 9 du RGPD qui interdit, en principe, le traitement des données biométriques, à moins que l'une des conditions de l'article 9.2 soit rencontrée. Attention, l'Autorité rappelle qu'il est nécessaire, mais qu'il ne suffit pas, de rencontrer une des conditions listées par l'article 9.2 pour que le traitement de données biométriques soit admissible. Encore faut-il s'assurer que ce traitement – qui constitue une ingérence dans le droit à la vie privée des personnes concernées – poursuive un objectif légitime, soit nécessaire et proportionné à cet objectif et qu'il respecte, en outre, les dispositions du RGPD.

reconnaissance faciale et le traitement de données biométriques qu'elle implique **peuvent engendrer des risques élevés pour les droits et libertés** des personnes concernées, en particulier en cas de fraude à l'identité. L'Autorité rappelle que **toute ingérence dans le droit à la protection des données à caractère personnel n'est admissible** que pour autant qu'elle poursuive **un objectif légitime**, qu'elle apparaisse **nécessaire** (c'est-à-dire qu'il ne doit pas exister de moyens moins intrusifs permettant d'atteindre l'objectif) et qu'elle soit **proportionnée** (c'est-à-dire que la mesure doit réaliser un juste équilibre entre les droits et intérêts en cause).

53. Par ailleurs, l'Autorité relève que **la comparaison faite avec l'utilisation de la biométrie qui permet de déverrouiller un smartphone est fallacieuse**. En effet, premièrement, au contraire de ce qui est prévu dans le projet, les données biométriques utilisées pour déverrouiller un smartphone sont gardées dans une enclave et ne quittent pas le smartphone[35]. Deuxièmement, au contraire de la photo conservée sur la carte d'identité, les smartphones ne stockent pas l'image complète du visage de la personne, mais uniquement des points caractéristiques ou des motifs, un sous-ensemble de caractéristiques extrait de l'image du visage de la personne concernée (« template ») ; ce qui réduit les risques de fraude à l'identité en cas de violation de ces données.

54. Ensuite, bien que la justification de l'amendement précise que « *les données biométriques ne seront en pratique pas conservées* », l'Autorité constate que **le dispositif de l'amendement ne reprend pas d'interdiction formelle de conserver les données biométriques au-delà de la comparaison**. Mais, même si une telle interdiction était effectivement reprise dans le dispositif du nouvel article 127 § 4 de la loi télécom et que sa violation était punie d'une sanction pénale spécifique et importante, il **existerait toujours un risque non-négligeable** que, à la suite d'une **fuite de données**[36], **des photos** utilisées dans le cadre de la comparaison entre les paramètres biométriques sur la photo du document d'identité de l'abonné et ceux de son visage **restent en circulation**. Au vu du risque élevé pour les droits et libertés (en particulier en cas de fraude à l'identité) qui découlerait d'une telle fuite de données (et de la circulation de telles photos), il convient de **limiter le recours à la reconnaissance faciale aux seules situations dans lesquelles cela apparait effectivement strictement nécessaire et proportionné**. Or, comme l'Autorité l'a déjà relevé dans son avis n° 108/2021, **le recours à la technologie faciale pour vérifier la fiabilité des données d'identification collectées en exécution du nouvel article 127 de la loi télécom n'apparait pas nécessaire**. En effet, il existe **d'autres moyens** d'authentification à distance qui sont **plus**

[35] Voyez, par exemple, *https://support.apple.com/en-gb/HT208108*

[36] Ou, plus précisément, d'une violation de données à caractère personnel au sens de l'article 4.12 du RGPD. Ce risque d'une fuite de données est d'autant plus important que, comme le souligne l'auteur de l'amendement lui-même, « *l'opérateur fera généralement appel à un ou plusieurs sous-traitants pour la mise en place de la solution de la comparaison faciale* ». Par ailleurs, l'Autorité relève que les individus ne peuvent pas vérifier que leur photo ne sera effectivement pas enregistrée, quand bien même une interdiction formelle serait reprise dans le dispositif, en particulier, parce que la reconnaissance faciale se fait à partir de moyens électroniques dont ils ne peuvent pas contrôler la configuration.

sécurisés que l'utilisation de la reconnaissance faciale, à savoir l'usage de l'eID[37] et le recours à des prestataires de services de confiance qualifiés qui offrent un service de signature électronique qualifiée (par exemple : Itsme). Ces deux outils offrent, en effet, un niveau de sécurité supérieur[38] à celui de la reconnaissance faciale **tout en permettant d'atteindre l'objectif poursuivi** qui est de veiller à la fiabilité de l'identification de la personne concernée. Lors de la remise de la carte d'identité électronique, un fonctionnaire communal vérifie que la personne à qui il remet cette carte d'identité électronique et les codes qui y sont associés – et qui permettent l'utilisation des modules d'authentification à distance – est bien la personne titulaire de cette carte (contrôle *de visu*). **À partir du moment où une méthode alternative moins intrusive** dans le droit à la protection des données à caractère personnel est disponible pour assurer la fiabilité des données d'identification collectées, **le législateur ne peut pas autoriser le recours à la reconnaissance faciale**[39]. Les garanties supplémentaires prévues par l'amendement ne changent rien à ce constat. En effet, le consentement de la personne concernée ne peut pas suffire à légitimer un traitement de données disproportionné. **L'amendement sera revu afin de supprimer la possibilité offerte aux opérateurs et canaux de vente de services de communications électroniques de recourir à une méthode automatique de comparaison entre les paramètres biométriques sur la photo du document d'identité de l'abonné et ceux de son visage[40]**.

[37] Dans la justification de l'amendement, l'auteur indique que « *Étant donné que la loi oblige les opérateurs à identifier leurs abonnés de manière fiable au bénéfice des autorités et qu'il convient d'éviter des fraudes en matière d'identité, il est essentiel de permettre aux opérateurs de pouvoir remplir ces tâches au moyen des méthodes d'identification les plus appropriées et fiables convenant au contexte de chaque canal numérique et à tous les groupes cibles. À titre d'exemple, la méthode proposée empêchera qu'une personne puisse s'identifier à l'aide d'une eID volé ou d'un passeport volé* » (c'est l'Autorité qui souligne). L'Autorité relève que l'usage de la carte eID permet à son titulaire de s'authentifier grâce à un code pin qui n'est, en principe, connu que de son titulaire. Au contraire de ce qu'avance le Gouvernement, le recours à code pin associée à l'utilisation de l'eID en vue de l'authentification de son titulaire empêche, en principe, qu'une personne puisse s'authentifier avec une carte eID volée, sans qu'il soit nécessaire de recourir à la reconnaissance faciale. En outre, toute carte eID volée ou perdue doit faire l'objet d'une déclaration de vol ou de perte. Cette déclaration peut être faite auprès de l'administration communale, de la police ou de l'helpdesk du Registre national (en pratique « Doc Stop » qui est accessible par Internet ou via un numéro gratuit). À la suite de cette déclaration, le document d'identité est « bloqué » (il est repris dans l'application CheckDoc) et le code pin de la carte est bloqué.

[38] Il y a, en effet, moins de risques qu'une fuite de données aboutisse à une fraude à l'identité.

[39] Dans la justification de l'amendement, l'auteur indique (en réponse à l'avis n° 108/2021 de l'Autorité) que *« Il est vrai que le client peut toujours revenir à des méthodes alternatives telles qu'ITSME et le lecteur eID, ainsi qu'à d'autres méthodes alternatives dans d'autres canaux de vente tels que le magasin physique. Toutefois, ces méthodes ne sont pas toujours les plus appropriées pour offrir une réponse dans chaque contexte numérique. L'identification sur la base de la comparaison faciale est complémentaire et constitue un complément nécessaire aux méthodes existantes. Il est ainsi difficile d'estimer la croissance que connaîtra la méthode ITSME. Celle-ci est facile d'utilisation mais nécessite une activation préalable, ce qui n'est pas le cas lors de l'utilisation des données biométriques. Les opérateurs estiment ainsi que les clients ne disposeront pas toujours d'ITSME.* […]. *De plus, l'utilisation des données biométriques est une solution pour les résidents non belges sans carte électronique belge pour étrangers ou pour les étrangers en visite en Belgique. L'eID et ITSME ne sont pas disponibles pour ces clients.* ». **L'Autorité n'est pas convaincue par l'argumentation selon laquelle, étant donné que les clients ne disposeront pas toujours d'Itsme, il convient d'autoriser le recours à la reconnaissance faciale pour assurer la fiabilité des données d'identification collectées.** Tout d'abord, force est constater que **l'introduction du Covid Safe Ticket** (CST) dans la vie quotidienne des personnes vivant en Belgique a amené une **grande partie de la population à installer Itsme sur son smartphone** afin d'y installer l'application CovidSafe.BE et d'y récupérer les certificats (de vaccination, de test ou de rétablissement) constituant le CST. Par ailleurs, **le fait que les personnes ne résidant pas en Belgique ne puissent pas installer Itsme ou s'authentifier par le biais d'une carte eID ne peut justifier le fait d'autoriser**, à l'égard de toute la population, **la mise en place d'un traitement de données qui n'apparait pas nécessaire et qui est dès lors disproportionné**. En effet, il existe pour ces personnes d'autres moyens de s'identifier (par exemple en se présentant à un point de vente).

[40] En tout état de cause, si malgré les considérations exprimées ci-dessus, l'auteur de l'amendement maintenait le recours à la reconnaissance faciale comme méthode de vérification de la fiabilité de l'identification de l'abonné, l'Autorité insiste pour que les opérateurs soient tenus de présenter une alternative à la reconnaissance faciale qui ne présente pas de barrières

5.2. Sur l'usage du code pin de la carte d'identité électronique belge (article 127 § 4, dernier alinéa)

55. Le nouvel article 127 § 4, dernier alinéa, prévoit que « *Lorsque l'abonné s'identifie à l'aide d'une carte d'identité électronique belge et que l'opérateur n'a pas mis en œuvre la méthode de comparaison faciale visée à l'alinéa 3, l'opérateur peut demander à l'abonné l'introduction du code PIN* ». Au vu des considérations qui précèdent, il convient de **supprimer les mots « *et que l'opérateur n'a pas mis en œuvre la méthode de comparaison faciale visée à l'alinéa 3* »** et de **remplacer le mot « *peut* » par le mot « *doit* »**. En effet, si l'objectif est de veiller à ce que les données d'identification collectées soient fiables, il est pertinent **d'exiger systématiquement** que les personnes qui présentent leur carte d'identité électronique **s'authentifie au moyen du code pin**.

6. À propos la liste des documents d'identification admis pour identifier l'abonné (article 127 § 5, alinéa 1er)

56. Le nouvel article 127 § 5, alinéa 1er, de la loi télécom liste les « *documents d'identification qui sont admis pour identifier l'abonné qui est une personne physique* ». L'Autorité **prend acte de la liste établie**.

7. À propos de la prise et de la conservation de copie de document d'identité par les opérateurs (article 127 § 5, alinéa 3)

57. Le nouvel article 127 § 5, alinéa 3, prévoit que « *Lorsqu'un opérateur identifie l'abonné à partir d'un document d'identification, il conserve une copie de ce document, sauf lorsqu'il s'agit de la carte d'identité électronique belge* ». Tout d'abord, l'Autorité rappelle **que la prise de copie de document d'identité génère nécessairement un risque élevé** pour les droits et libertés des personnes concernées au vu des conséquences potentiellement graves d'une fuite de données se rapportant à ces documents (fraude à l'identité)[41]. C'est pourquoi il est nécessaire de **limiter au maximum toute prise de copie de documents d'identité**. Dans la mesure où il existe une solution technologique qui permet d'extraire, de manière électronique et fiable, de la carte d'identité électronique, des données relatives à l'identité civile de la personne physique, il n'est pas nécessaire de faire et de conserver une copie de cette carte d'identité. À ce propos, **l'Autorité prend acte** du fait que l'amendement prévoit déjà que les Belges doivent, en principe, s'identifier à l'aide de leur carte d'identité électronique[42] et

supplémentaires significatives de telle sorte que cette alternative ne pourrait pas être considérée comme une véritable alternative permettant d'assurer le caractère libre du consentement.

[41] Voyez, à ce propos, la Recommandation d'initiative de la Commission de la protection de la vie privée (prédécesseur en droit de l'Autorité) relative à la prise de copie des cartes d'identité ainsi qu'à leur utilisation et à leur lecture électronique, Recommandation n° 03/2011 du 25 mai 2011.

[42] Dans la justification de l'amendement, l'auteur indique que *« En principe, un Belge doit s'identifier en Belgique à l'aide de sa carte d'identité électronique belge et non à l'aide de son passeport international* ». Cette obligation est traduite dans le dispositif par le fait que les Belges ne peuvent s'identifier avec leur passeport uniquement pour les services de communications

interdit la conservation d'une copie de la carte d'identité électronique belge. Toutefois, **afin d'éviter toute prise de copie de la carte d'identité belge**, il convient de mettre en place une solution technologique qui garantisse que les données d'identité du titulaire d'une carte d'identité électronique soient extraites en vue de leur insertion directe dans la base de données que les opérateurs doivent établir en exécution du nouvel article 127 de la loi télécom. **Concernant les autres documents d'identité** dont on ne peut pas extraire les données d'identification de manière électronique et fiable, l'amendement prévoit que l'opérateur doit conserver une copie de ce document. Dans la justification de l'amendement, le Gouvernement indique que la conservation d'une copie de ces documents se justifie « *parce que les opérateurs sont moins familiers avec les cartes d'identité étrangères et les passeports étrangers* ». **Cette motivation ne convainc pas l'Autorité de la nécessité de prendre une copie de ces documents d'identité**. Au vu du risque important de vol d'identité que génère la circulation de copies de documents d'identité, il convient, en lieu et place de la conservation de telles copies, **de prévoir uniquement la mention**, dans la base de données établie par les opérateurs en vertu de l'article 127 de la loi télécom, **des données d'identité collectées à partir de la consultation des documents d'identité**. **L'article 127 § 5, alinéa 3, sera supprimé**[43].

8. À propos de l'autorisation d'exiger des factures de fournisseurs de différents produits et d'autres informations complémentaires pour assurer la fiabilité de l'identité de l'abonné (article 127 § 5, alinéas 4 et 5)

58. Le nouvel article 127 § 5, alinéas 4 et 5, prévoit que « *Lorsque l'abonné soumet un document d'identification visé à l'alinéa 1er pour s'identifier et que l'opérateur n'est pas en mesure d'assurer la fiabilité de l'identité de l'abonné sur base de ce document, il peut demander à l'abonné, afin de renforcer cette fiabilité, de lui communiquer :*
    - *des factures de fournisseurs de différents produits ou services, pour les services de communications électroniques qui sont payés après leur fourniture*
    - *des informations complémentaires.*

    L'opérateur conserve une copie de ces factures et de ces informations ».

59. Dans la justification de l'amendement, l'auteur indique que *« Vu la difficulté pour les opérateurs de détecter les documents d'identité qui seraient falsifiés, ces derniers demandent parfois à l'abonné de leur fournir des factures d'entreprises reconnues d'utilité publique (par exemple des fournisseurs d'eau, de gaz ou d'électricité). Un opérateur a en effet un intérêt commercial à correctement identifier son*

électroniques payés avant leur fourniture. Pour tous les services « postpaid », les belges ne pourront s'identifier qu'avec leur carte d'identité électronique.

[43] Si, toutefois, malgré les considérations émises ci-dessus, le Gouvernement maintenait l'obligation de conserver une copie des documents d'identité qui ne sont pas une carte d'identité électronique belge, l'Autorité insiste pour que – conformément à la recommandation 3/2011 de la CPVP – le dispositif de l'amendement prévoit, au moins, que la copie du document d'identité soit barrée et que la finalité de la copie soit indiquée sur la copie, et ce afin d'éviter toute reproduction conforme de la carte et de limiter toute utilisation pour des finalités détournées

abonné et à éviter des fraudes en matière d'identité. Il est important que la fiabilité de l'identification de l'abonné pour les besoins des autorités soit au même niveau que la fiabilité de cette identification pour les besoins commerciaux de l'opérateur ».

60. L'Autorité constate qu'une **telle disposition va au-delà de ce qui est nécessaire dans une société démocratique** en ce qu'elle aboutit à autoriser des traitements de données potentiellement disproportionnés et discriminatoire.

61. Tout d'abord, l'Autorité relève que, telle que rédigée, **la disposition n'est pas suffisamment précise et prévisible** pour répondre à l'exigence du principe de légalité. En effet, la disposition ne précise pas les circonstances dans lesquelles l'opérateur n'est pas en mesure d'assurer la fiabilité de l'identité de l'abonné. Qu'est-ce qui est visé par-là ? Est-ce que cela vise toute situation dans laquelle une personne présente un document d'identité pour lequel il n'y pas de code pin ? Est-ce que cela vise la situation dans laquelle la personne qui vérifie, au nom de l'opérateur, le document d'identité estime, de manière subjective (mais comment peut-il en être autrement si la disposition ne donne aucun critère objectif ?), ne pas être en mesure d'assurer la fiabilité de l'identité de l'abonné ? Quand une personne est-t-elle en mesure d'assurer la fiabilité de l'identité de l'abonné ? **La disposition en projet ne détermine pas avec suffisamment de prévisibilité les conditions et les circonstances dans lesquelles le traitement de données à caractère personnel qu'elle autorise peut avoir lieu**.

62. En outre, **les informations** qui peuvent être exigées par l'opérateur ne sont pas, non plus, **définies de manière claire et prévisible**. D'une part, il est question des « *factures de fournisseurs de différents produits ou service*s ». De quels produits et services est-il question ? De combien de facture est-il question ? D'autre part, la disposition en projet mentionne « *des informations complémentaires* » sans aucune autre précision. **L'absence de clarté des termes utilisés porte également atteinte au principe de légalité.**

63. De plus, la disposition en projet indique que l'opérateur « peut demander » (et non pas « doit demander ») des documents complémentaires s'il n'est pas en mesure d'assurer la fiabilité de l'identité de l'abonné. Or, aux termes du principe de légalité, **c'est au législateur qu'il revient de déterminer**, dans le respect des principes de nécessité, de proportionnalité et de non-discrimination, **les conditions dans lesquelles des documents complémentaires doivent être collectés et conserver pour assurer la fiabilité de l'identification**. En outre, le traitement de données qui consiste à collecter et à conserver ces informations et documents complémentaires en vue de renforcer la fiabilité de l'identification de l'abonné pour les besoins des autorités ne **sera licite, au sens de l'article 6 du RGPD, que s'il est nécessaire au respect d'une obligation légale** à laquelle le responsable du traitement est soumis (article 6.1.c) du RGPD). En effet, aucune autre base de licéité de l'article 6 du RGPD ne pourrait être invoquée pour légitimer les traitements de données réalisés

dans ce contexte. **Or, pour qu'il y ait une obligation légale au sens de l'article 6.1.c) du RGPD, il faut que le responsable du traitement** (à savoir, en l'occurrence les opérateurs) **n'ait pas le choix de se conformer ou non à l'obligation**[44].

64. En outre, **l'absence de clarté** concernant **les circonstances** dans lesquelles l'opérateur peut exiger d'autres documents que les documents d'identité et **les documents et informations qui peuvent être exigés** dans ce contexte **est susceptible de générer une application discriminatoire de la loi**. En effet, il est probable que certaines catégories de la population se voient beaucoup plus systématiquement que d'autres demander des informations complémentaires afin de justifier la fiabilité de leur document d'identité ; et ce sans que cela soit justifié et proportionné à l'objectif poursuivi. De même, il est possible que les opérateurs soient plus « exigeants » pour certaines catégories de la population que pour d'autres à propos des documents et informations à fournir pour assurer la fiabilité de leur identification ; et ce, à nouveau, sans justification. En effet, **aucune garantie n'est introduite dans la loi pour éviter le traitement discriminatoire de certaines catégories de la population**. Certes, les opérateurs sont soumis à la loi du 10 mai 2007 tendant à lutter contre certaines formes de discrimination, laquelle interdit les discriminations dans l'accès aux biens et services et la fourniture de biens et services à la disposition du public. Toutefois, **il est essentiel que les règlementations qui encadrent spécifiquement des traitements de données à caractère personnel, en particulier les traitements qui sont nécessaires au respect d'une obligation légale à laquelle le responsable du traitement est soumis, comme c'est le cas en l'espèce, soient rédigées de manière telle qu'elles évitent que lesdits traitements de données puissent avoir un effet discriminatoire à l'égard des personnes physiques concernées**.

65. Par ailleurs, et plus fondamentalement encore, **l'Autorité doute de la nécessité et de la proportionnalité** de l'ingérence causée dans le droit à la protection des données à caractère personnel par **la collecte et la conservation des factures de fournisseurs de différents produits ou services et d'autres informations complémentaires afin d'assurer la fiabilité de l'identité de l'abonné[45]**. Les éléments avancés dans la justification de l'amendement ne permettent pas de comprendre pourquoi il est nécessaire et proportionné d'exiger, outre un document d'identité, des factures de produits ou de services ou d'autres informations pour assurer la fiabilité de l'identification. **Or, au vu de l'ingérence importante causé par une telle collecte et conservation d'informations complémentaires et des risques de cette mesure pour les droits et libertés des personnes concernées**, en particulier de discrimination, **il appartient au**

[44] Groupe de travail « Article 29 » sur la protection des données (prédécesseur du Comité européen de la protection des données), *Avis n° 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE,* adopté le 9 avril 2014, WP 217, p. 21-22.

[45] À ce propos, l'Autorité relève que la disposition pourrait aboutir à une collecte large d'information. Qu'il suffise de penser au cas d'une personne majeure qui vit avec ses parents et dont tous les factures d'eau, de gaz et d'électricité sont au nom de l'un de ses parents. Afin d'assurer la fiabilité de son identité, cette personne devra-t-elle fournir, non seulement lesdites factures, mais également une composition de ménage ?

législateur de démontrer, à l'aide d'éléments factuels et concrets, que le traitement de données envisagés est bien nécessaire et proportionné. Tel n'est actuellement pas le cas.

66. **Au vu de l'ensemble des considérations émises ci-dessus, les alinéas 4 et 5 du nouvel article 127 § 5 seront supprimés**.

9. À propos de la délégation au Roi d'autoriser certaines méthodes d'identification spécifiques (article 127 § 5, dernier alinéa)

67. Le nouvel article 127 § 5, dernier alinéa, prévoit que « *Le Roi peut autoriser certaines méthodes d'identification spécifiques, le cas échéant indirectes, pour les personnes qui ne disposent d'aucun des documents visés à l'alinéa 1er* ». L'Autorité **prend note de cette délégation de compétence**. Elle attire d'ores et déjà l'attention du Roi sur le fait que **ces méthodes d'identification devront respecter le principe de nécessité et de proportionnalité**.

10. À propos des données d'identifications qui doivent être conservées par les opérateurs (article 127 § 6)

68. Le nouvel article 127 § 6 de la loi télécom détermine la **liste maximale** des données d'identification ainsi que la **liste minimale** des données d'identification qui doivent être conservées par l'opérateur qui identifie l'abonné par le biais d'une méthode d'identification directe. **L'Autorité a plusieurs remarques à propos de ces deux listes de données** : une première remarque à propos du principe des deux listes de données à conserver et des remarques plus ponctuelles sur le respect du principe de minimisation des données.

69. Premièrement, l'Autorité rappelle que **la base de licéité du traitement** qui consiste en l'identification des abonnés et en la conservation de leurs données d'identification est le respect d'une **obligation légale** à laquelle le responsable du traitement est soumis (article 6.1.c) du RGPD). Or, comme l'Autorité l'a déjà relevé plus haut dans son avis, pour qu'il y ait une obligation légale au sens de l'article 6.1.c) du RGPD, il **faut que le responsable du traitement** (à savoir, en l'occurrence les opérateurs) **n'ait pas de marge d'appréciation quant à la façon de se conformer à l'obligation légale**[46]. **Donner aux opérateurs le choix de conserver certaines données d'identification** (sans les y contraindre) n'est **pas admissible** au regard du fait que la collecte et la conservation des données d'identification n'est licite que **dans la mesure où le traitement de données est nécessaire au respect d'une obligation légale** à laquelle ils sont soumis. Il s'ensuit que **le législateur doit déterminer les données d'identification à conserver dans une liste unique**, quitte à préciser

[46] Groupe de travail « Article 29 » sur la protection des données (prédécesseur du Comité européen de la protection des données), *Avis n° 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE,* adopté le 9 avril 2014, WP 217, p. 21-22.

que certaines données ne doivent être conservées que dans la mesure où elles existent pour la personne concernée (comme, par exemple, le numéro de registre national). **L'amendement sera modifié sur ce point**.

70. Ensuite, des **remarques plus ponctuelles** sur la conformité des données à conserver avec l'exigence selon laquelle ces données doivent être « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données)* » :

a) On retrouve dans la liste maximale des données qui peuvent être conservées « *la photo de l'abonné mais uniquement pour les documents d'identité autres que la carte d'identité électronique belge* » (article 127 § 6, alinéa 1er, 5°). L'Autorité rappelle que, conformément à l'article 6 § 4 de la loi du 19 juillet 1991 relative aux registres de la population, aux cartes d'identité, aux cartes des étrangers et aux documents de séjour (ci-après « la loi du 19 juillet 1991 »), l'utilisation de la photographie du titulaire d'une carte d'identité n'est licite que « si *cette utilisation est autorisée par ou en vertu d'une loi, d'un décret ou d'une ordonnance* ». Cette condition posée à l'utilisation de la photographie du titulaire d'une carte d'identité montre bien que le législateur a estimé que le traitement de cette donnée comportait des risques particuliers pour la personne concernée[47]. La photographie qui se retrouve sur la carte d'identité – ou tout autre document d'identité – constitue, en effet, une **donnée biométrique** dans la mesure où elle est utilisée selon un mode technique spécifique permettant l'identification ou l'authentification unique d'une personne physique. Conformément à l'article 9.2.g) du RGPD, le traitement de la photographie qui est reprise sur un document d'identité ne serait licite – dans le contexte de l'amendement examiné – que dans la mesure où il est nécessaire « *pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée* ». Au vu des risques pour les droits et libertés des personnes concernées, **l'Autorité n'aperçoit pas pourquoi la collecte et la conservation de la photo du titulaire d'un autre document d'identification serait nécessaire et proportionné à l'objectif d'intérêt public poursuivi.** En l'absence de justification adéquate et convaincante quant à la nécessité et à la proportionnalité de la collecte et de la conservation de cette donnée, **cette donnée sera dès lors supprimée de la liste maximale des données qui peuvent (ou doivent) être conservées.**

[47] Dans l'Exposé des motifs du projet de loi portant des dispositions diverses concernant le Registre national et les registres de population, il est indiqué que *« Par contre, le projet de loi précise que la photographie de la carte d'identité doit être traitée comme le numéro de Registre national et les empreintes digitales, à savoir qu'elle ne peut pas faire l'objet d'un traitement, à savoir ni enregistrée, ni utilisée (cf. point 74). Cependant, dans la mesure où la photographie est également directement visible à l'œil nu, le même procédé de protection que celui appliqué aux empreintes digitales ne saurait être adopté* » (54-3256/001, p. 39).

b) L'Autorité relève que **l'adresse du domicile, l'adresse email et le numéro de téléphone** (article 127 § 6, alinéa 1er, 6°) ne constituent pas des données d'identification mais **des données de contact**. Elles **ne doivent donc pas être reprises dans la liste des données d'identification** qui doivent être conservées par les opérateurs.

c) Le notion de « ***numéro de sécurité publique*** » (article 127 § 6, alinéa 1er, 8°) **doit être définie.** S'il s'agit du « *numéro de dossier attribué par l'Office des Etrangers* » qui est visé à l'article 2 de l'arrêté royal du 16 juillet 1992 déterminant les informations mentionnées dans les registres de la population et dans le registre des étrangers, il convient de l'indiquer.

d) L'Autorité rappelle que, selon la jurisprudence de l'ancien Comité sectoriel du Registre national, **le numéro de Registre national**, combiné au nom et au prénom, **permet une identification plus exacte que le numéro de carte d'identité**. En outre, la Commission de la protection de la vie privée, prédécesseur en droit de l'Autorité de protection des données, soulignait déjà que le numéro de la carte d'identité ne convient pas comme identifiant car il n'est pas stable dans le temps. Dans cette mesure, l'Autorité estime que si l'opérateur conserve déjà le numéro de registre national, il ne peut pas conserver – en outre – le numéro de la carte d'identité**. La liste sera amendée afin de préciser que le numéro du document ne peut être conservé que dans la situation où l'opérateur ne dispose déjà du numéro de registre nationa**l.

e) Dans la liste des données à conserver au minimum, il est indiqué que *« si l'opérateur identifie son abonné à partir des données disponibles sur sa carte d'identité électronique belge : le numéro de registre national, le nom et le prénom* » (article 127 § 6, alinéa 2, 1er tiret). Ces éléments permettent effectivement une identification certaine de l'abonné. **L'Autorité estime dès lors que seules ces données peuvent être conservées par les opérateurs en exécution de l'article 127 de la loi télécom lorsque l'abonné est identifié à partir d'une carte d'identité électronique belge**.

f) La **délégation au Roi donnée par l'article 127 § 6, alinéa 2,** deuxième tiret de déterminer les données (outre le nom, prénom et la date de naissance) que l'opérateur doit conserver (au minimum) n'est **pas conforme au principe de légalité**, tel qu'il a été interprété dans l'arrêt de la Cour constitutionnelle n° 158/2021.

71. **La liste des données d'identification qui doivent être conservées par les opérateurs sera adaptée afin de répondre aux différentes remarques émises ci-dessus**.

11. À propos des méthodes d'identification indirecte (article 127 § 9)

72. Le nouvel article 127 § 9 de la loi télécom détermine les **différentes méthodes indirectes** par lesquelles les opérateurs doivent permettre aux autorités d'identifier leurs abonnés. Il s'agit d'une identification :

(1) par la **conservation de l'adresse IP ayant servi à la création du compte** qui permet l'utilisation du service de communications électroniques et **des adresses IP à la source de la connexion**, l'horodatage ainsi que, en cas d'utilisation partagée d'une adresse IP de l'utilisateur final, des ports qui lui ont été attribués ;

(2) par la collecte et la conservation du **numéro de téléphone** de l'abonné attribué dans le cadre d'un service de communications électroniques payant pour lequel un opérateur doit identifier l'abonné conformément au présent article ;

(3) en cas de **paiement électronique en ligne** spécifique à la souscription d'un service de communications électroniques, par la collecte et la conservation de la **référence de l'opération de paiement, le nom, le prénom, le lieu et la date de naissance** de l'abonné qui est une personne physique ou qui agit pour le compte d'un abonné qui est une personne morale afin de remplir ses obligations en matière d'identification ;

(4) en cas de souscription à un service de communications électroniques mobiles fourni au moyen d'une carte prépayée d'un abonné qui réside dans un **centre fermé ou un lieu d'hébergement pour étrangers**, par la collecte et la conservation du nom et du prénom de l'abonné, son numéro de sécurité publique et les coordonnées du centre ou du lieu d'hébergement où la souscription a eu lieu ;

(5) par la collecte et la conservation **des données fixées par le Roi** pour (1) les services de communications électroniques utilisés à titre occasionnel par les abonnés, pour lesquels une méthode d'identification directe implique des contraintes importantes pour les abonnés et les opérateurs et pour lesquels une méthode d'identification indirecte permet aux autorités légalement habilitées d'identifier l'abonné de manière fiable et pour (2) les services de communications électroniques déterminés par le Roi, fournis à des personnes qui ne disposent d'aucun des documents d'identité visés par le nouvel article 127 § 5.

73. Tout d'abord, comme l'Autorité l'a déjà souligné plus haut dans son avis, elle relève, à nouveau, que **la qualité des données** d'identification recueillies par le biais d'une méthode d'identification indirecte **apparait incertaine** et ne garantit pas que la personne qui sera identifiée est bien la personne qui

aura effectivement utilisé le service de communications électroniques. **L'Autorité insiste pour que les parlementaires évaluent la nécessité et la proportionnalité de l'ingérence dans le droit à la protection des données à caractère personnel par la collecte des données nécessaires à l'identification indirecte des abonnés à l'aune de l'incertitude concernant la qualité de ces données pour atteindre l'objectif poursuivi**, à savoir assurer une identification fiable de l'utilisateur final.

74. Ensuite, l'Autorité constate que **certaines méthodes d'identification indirecte semblent nouvelles** (c'est le cas pour les méthodes reprises sous les (1) et (2) ci-dessus) alors que **d'autres méthodes d'identification indirecte étaient déjà utilisées** afin d'identifier l'utilisateur final de services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée (c'est le cas pour les méthodes (3)[48] et (4)[49] ci-dessus). **L'amendement étend toutefois les catégories d'autorités qui peuvent avoir recours à ces méthodes d'identification indirecte**. Jusqu'à présent, seuls les services de renseignements et de sécurité pouvaient, sans équivoque[50], identifier un utilisateur final à partir de la référence de l'opération de paiement[51]. Comme la justification de l'amendement l'indique, *« Pour s'assurer que la méthode d'identification indirecte visée à l'alinéa 1er, 3°, fonctionne en pratique, la possibilité de requérir des données d'identification d'un fournisseur de service de paiement, […] est étendue aux autres autorités belges qui sont habilitées à obtenir de l'opérateur télécom l'identité de l'abonné. Si ces autorités peuvent obtenir cette identité de l'opérateur télécom, elles doivent aussi pouvoir l'obtenir d'un fournisseur de service de paiement (identification sur base de la référence d'une transaction bancaire conservée par l'opérateur) selon les mêmes modalités, sauf si la législation organique de l'autorité prévoit d'autres modalités. Cela vaut également dans le cadre du contrôle par l'IBPT du respect de l'article 127 de la loi télécom* ». L'Autorité rappelle que **la nécessité et la proportionnalité de cette extension doit être justifiée à l'aide d'éléments factuels et concrets**. La justification de l'amendement n'apporte pourtant aucun élément factuel et concret permettant de constater le caractère nécessaire et proportionné de l'extension des catégories d'autorités pouvant avoir accès à l'identité d'un abonné à un service de communications électroniques alors que cette extension augmente l'ingérence dans le droit au respect de la vie privée et le droit à la protection des données à caractère personnel de tous les abonnés de

[48] Voyez l'article 17 de l'arrêté royal du 27 novembre 2016 relatif à l'identification de l'utilisateur final de services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée.
[49] Voyez l'arrêté ministériel désignant en tant qu'autorité publique l'Office des étrangers du SPF Intérieur conformément à l'article 9, alinéa 2, de l'arrêté royal du 27 novembre 2016 relatif à l'identification de l'utilisateur final de services de communications électroniques publics mobiles fournis sur la base d'une carte prépayée
[50] Dans la justification de l'amendement n° 16, le Gouvernement indique que l'article 46bis du C.I.C, qui est la base légale qui permet au Procureur du Roi de procéder à l'identification de l'abonné ou de l'utilisateur habituel d'un service de communications électroniques, « fournit déjà une base légale pour procéder à l'identification indirecte visée à l'article 127 de la loi relative aux communications électroniques », mais qu'il est « d'avis que cette possibilité doit être plus précisée dans les lois organiques des autorités qui souhaitent faire usage de ces méthodes d'identification indirecte. L'article 46bis du Code d'instruction criminelle sera donc également modifié ». L'Autorité constate que la lecture de l'article 46bis du C.I.C ne laisse pas clairement entrevoir le pouvoir du Procureur du Roi d'exiger des institutions financières de révéler l'identité de la personne « derrière » la référence d'une transaction bancaire électronique.
[51] Cette méthode est en effet prévue par l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

services de communications électroniques. Cette extension sera supprimée ou son caractère nécessaire et proportionné sera justifié à l'aide d'éléments factuels et concrets.

75. Par ailleurs, l'Autorité a **plusieurs remarques** à formuler à propos des données collectées dans le cadre des méthodes d'identification indirecte.

76. Tout d'abord, à propos de la collecte de données en cas de paiement électronique en ligne, l'Autorité constate que la collecte de la date et du lieu de naissance va au-delà de ce qui est nécessaire pour atteindre la finalité d'identification indirecte et est dès lors contraire à l'article 5.1.c) du RGPD. **L'amendement sera revu afin de supprimer l'obligation de collecter ces deux données.**

77. Ensuite, à propos de **la collecte des adresses IP comme méthodes d'identification indirecte** :

- Premièrement, l'Autorité constate que **la collecte et la conservation de l'adresse IP ayant servi à la création du compte** qui permet l'utilisation du service de communications électroniques **doit déjà être collectée et conservée**, pour la même durée, **en vertu du nouvel article 126 § 1, 4°** (introduit par l'amendement n° 1). L'Autorité se demande dès lors pourquoi la même donnée doit être collectée en vertu de l'article 127.

- Deuxièmement, l'Autorité relève qu'il est assez facile pour un utilisateur de contourner cette méthode d'identification indirecte, par exemple, en souscrivant au service de communications électroniques ou en l'utilisant par le biais d'un réseau wifi public ou ouvert ou en ayant recours à Tor. Dans ces conditions, l'Autorité est d'avis que la collecte et la conservation de l'adresse IP ayant servi à la création du compte et des adresses IP attribuées à la source de la connexion ne permettent pas systématiquement de rencontrer adéquatement l'objectif poursuivi. L'Autorité s'interroge dès lors sur la pertinence (et donc la nécessité) de la mesure. L'Autorité invite les parlementaires à évaluer – et à le justifier, le cas échéant – si la mesure est effectivement pertinente et nécessaire pour atteindre l'objectif qu'ils veulent poursuivre.

- Troisièmement, **l'Autorité se demande si l'objectif de la collecte et de la conservation des adresses IP à la source de la connexion est bien d'imposer la collecte et la conservation de toutes les adresses IP qui utilisent le service de communications électroniques**. Si tel est le cas, l'amendement imposerait aux opérateurs qui décident d'avoir recours à cette méthode d'identification indirecte **une obligation de conservation généralisée et indifférenciée d'une donnée de trafic**, à savoir les adresses IP des équipements qui se connectent à un service de communications électroniques ; ce qui constituerait **une ingérence** dans le droit à la vie privée des personnes concernées qui devrait, à l'estime de l'Autorité, **être qualifiée d'importante**, notamment parce qu'elle permet de déterminer la fréquence d'utilisation

d'un service de communications électroniques (ce qui va au-delà de la question de savoir l'identité de la personne qui est abonné audit service) et de déduire des informations relatives à la localisation de l'utilisateur du service (en particulier s'il s'agit de services de messagerie)[52]. L'Autorité constate, en outre, que **les données collectées en vertu de l'article 127**, et donc les adresses IP attribuées à la source de la connexion qui utilisent un service de communications électroniques, **doivent être conservées pendant 12 mois après la fin du contrat** (voyez le nouvel article 127 § 3, alinéa 3). **Une telle durée de conservation** pour toutes les adresses IP qui se sont connectés à un service de communications électroniques **est excessive et disproportionnée**. **L'amendement sera adapté** afin de limiter **la durée de conservation** des adresses IP qui se connectent à un service de communications électroniques **à 12 mois après la fin de la session,** conformément à ce qui est prévu par le nouvel article 126 de la loi télécom, et non pas 12 mois après la fin du service.

- Enfin, l'Autorité **s'interroge**, plus largement, **sur la pertinence de la conservation au-delà de 12 mois après la fin de la session de l'adresse IP ayant servi à la création du compte et des adresses IP attribuées à la source de la connexion** pour identifier les abonnés à un service de communications électroniques gratuit, étant donné que 12 mois après la fin de la session, il semblerait qu'il ne soit plus possible d'identifier la personne à qui l'adresse IP ayant servi à la création du compte ou l'adresse IP utilisée pour se connecter au service de communications électroniques a été attribuée. En effet, les fournisseurs d'accès à Internet, qui attribuent les adresses IP, doivent conserver les adresses IP attribuées à la source d'une connexion pendant 12 mois après la fin de la session. Si une personne souscrit à un service de communications électroniques gratuit par internet, l'opérateur de ce service conservera l'adresse IP à partir de laquelle le compte (voire toutes les adresses IP qui se sont connectées à ce service) a été créé ; et ce en vue de rencontrer son obligation d'identifier – ou au moins de permettre l'identification par les autorités – tous ses abonnés. Mais pour pouvoir effectivement identifier cette personne, les autorités devront, non seulement collecter l'adresse IP ayant servi à la création du compte ou s'étant connecté au service de communications électroniques auprès de l'opérateur dudit service, mais elles devront ensuite demander au fournisseur d'accès à internet l'identité de l'abonné à qui cette adresse IP a été attribuée au moment auquel le compte a été créé ou au moment où le service a été utilisé. Or, si l'attribution a eu lieu il y a plus de 12 mois, le fournisseur d'accès à Internet n'aura plus accès à cette information et les autorités ne pourront pas connaitre. Dans ces conditions, et au vu de la gravité de l'ingérence causée par la conservation généralisée des

[52] En effet, il existe plusieurs techniques qui permettent de déduire, à partir d'une adresse IP, la localisation de l'équipement terminal à qui cette adresse IP a été attribuée (et donc la localisation de son utilisateur). Il existe même des services facilement accessibles sur Internet qui permettent de localiser un appareil (et la personne qui l'utilise) à partir de son adresse IP (voyez, par exemple, https://www.ip2location.com/, https://iplocation.com/, https://www.home.neustar/resources/tools/ip-geolocation-lookup-tool). Les grands acteurs, tels que Google ou Apple, connaissent la localisation de nombreuses adresses IP (tous les appareils mobiles dotés de services de localisation) et peuvent localiser d'autres adresses IP s'ils disposent d'informations sur les SSID Wifi ou les balises BLE que l'appareil peut voir.

adresses IP, l'Autorité considère que l'amendement doit être modifié afin d'y préciser que les adresses IP ayant servi à la création du compte et des adresses IP attribuées à la source de la connexion, qui sont utilisées comme méthode d'identification indirecte, **doivent être conservées pendant 12 mois après la fin de la session** (et non pendant 12 mois après la fin du service)

12. À propos de la présomption réfragable selon laquelle l'abonné à un service de communications électroniques est présumé utiliser lui-même ce service (article 127 § 10, alinéa 1er)

78. Le nouvel article 127 § 10, alinéa 1er, établit une **présomption réfragable** selon laquelle « *la personne identifiée est présumée utiliser elle-même le service de communications électroniques* ». Comme l'Autorité l'a déjà relevé plus haut dans son avis, dans les faits, **il n'est pas rare que l'utilisateur d'un service de communications électroniques soit différent de la personne ayant souscrit à ce service**. En effet, les abonnés peuvent autoriser une autre personne à utiliser un service de communications électroniques auquel ils ont souscrit (en particulier un service d'accès à un Internet ou un service de téléphonie fixe ou mobile). Les services de communications électroniques, en particulier ceux du type « OTT », peuvent faire l'objet d'un **hacking sans que la personne concernée s'en soit rendu compte.** Un réseau wifi peut également faire l'objet de hacking ou être partagé entre plusieurs utilisateurs (notamment en cas de réseau wifi « ouvert » ou de mise à disposition d'un réseau wifi dans un café). Par ailleurs, une personne peut perdre ou se faire voler son téléphone mobile et ne s'en rendre compte que plusieurs jours après les faits. En effet, le législateur ne peut pas supposer que le propriétaire d'une carte SIM sait en tout temps où cette carte SIM se trouve. Au contraire de ce qui existe pour la carte d'identité[53], il **n'existe pas d'obligation légale d'être porteur de la (des) carte(s) SIM dont on est propriétaire**. Certes, la présomption est réfragable et la personne peut la contester par toute voie, mais il faut tenir compte du fait **qu'il peut être extrêmement difficile, voire impossible, d'apporter une preuve négative** (à savoir le fait que la personne identifiée n'est pas celle qui a utilisé le service de communications électroniques). **L'Autorité invite dès lors les parlementaires à être extrêmement prudents avant de maintenir (et d'étendre) une telle présomption en droit positif**.

[53] Article 6 § 7 de la loi du 19 juillet 1991 et article 1er de l'arrêté royal du 25 février 2003 relatif aux cartes d'identité.

13. À propos des les conditions auxquelles une personne morale peut souscrire à un service de communications électroniques au nom et pour le compte de personnes physiques qui sont les abonnés (article 127 § 10, alinéa 2)

79. Le nouvel article 127 § 10, alinéa 2, fixe les conditions auxquelles une personne morale peut souscrire à un service de communications électroniques au nom et pour le compte de personnes physiques qui sont les abonnés.

80. La première condition est que la personne morale s'identifie auprès de l'opérateur conformément au nouvel article 127 § 7. L'Autorité **en prend acte**.

81. Les deuxième et troisième conditions sont que la personne morale *« conserve une liste actualisée permettant de faire le lien entre le service de communications électroniques et les abonnés, comprenant au minimum le nom, le prénom et le numéro de registre national de l'abonné* » et « *qu'elle identifie les abonnés à l'aide d'un des documents d'identité visés au paragraphe 5 [qui liste les documents d'identité avec lesquelles une personne peut être identifiée], conformément aux exigences de fiabilité visées au paragraphe 4, alinéa 1er et 2* ». **L'Autorité prend acte de ces deux obligations** qui pèsent sur les personnes morales qui souscrivent à un service de communications électroniques pour le compte d'une personne physique.

82. La quatrième obligation consiste à fournir « *à l'opérateur une copie du document d'identification des abonnés, sauf lorsqu'il s'agit de la carte d'identité électronique belge, conformément au paragraphe 5, alinéa 3* ». **Pour une identité de motifs à ceux exprimés lors de l'examen de l'article 127 § 5, alinéa 3, l'Autorité estime que cette quatrième obligation doit être supprimée**.

83. Le nouvel article 127 § 10, alinéa 3, détermine la durée pendant laquelle la personne morale doit conserver les données relatives à un abonné dans la liste actualisée : 12 mois après la fin du service de communications électroniques. **L'Autorité en prend note**.

14. À propos de l'obligation de conserver le numéro de châssis du véhicule dans lequel une de ses cartes SIM ou toute carte équivalente a été intégrée (article 127 § 10, alinéa 3)

84. Le **nouvel article 127 § 10, alinéa 5**, impose à l'opérateur de conserver « *le numéro de châssis du véhicule dans lequel une de ses cartes SIM ou toute carte équivalente a été intégrée, ainsi que lien entre le numéro de châssis et le numéro de cette carte, à partir de la date d'activation du service de communications électroniques jusqu'à douze mois après la fin du service* », étant entendu que *« Le Roi peut fixer les modalités de l'obligation visée à l'alinéa 3 et peut imposer aux entreprises qui disposent du numéro de châssis de le transmettre aux opérateurs* ».

85. Cette **nouvelle obligation** de conservation d'une nouvelle donnée par les opérateurs est **justifiée comme suit** : « *L'évolution montre qu'il est (de plus en plus) difficile pour les autorités d'exploiter les services de communications électroniques dans leurs enquêtes. Dans certains cas, un abonné parvient à s'identifier sous une fausse identité auprès de l'opérateur. La jurisprudence de la CJUE a fortement réduit la possibilité d'imposer aux opérateurs de conserver des métadonnées de manière généralisée et indifférenciée. Il est de plus en plus difficile pour les autorités judiciaires et les services de renseignement et de sécurité d'avoir accès au contenu des communications, vu la mise en place de la 5G et la généralisation de systèmes d'encryptage de bout en bout. Il est donc essentiel de permettre aux autorités judiciaires et aux services de renseignements et de sécurité de bénéficier des nouvelles opportunités qu'offrent l'évolution des technologies. C'est dans ce cadre qu'il est prévu que les opérateurs doivent conserver les numéros de cartes SIM qui sont intégrées dans des véhicules connectées en faisant le lien avec le numéro de châssis de ces véhicules. Cette obligation concrétise une proposition des opérateurs eux-mêmes. L'identification de la société avec laquelle l'opérateur a contracté (l'abonné) ne sera pas suffisante pour les services de sécurité, qui chercheront à connaître l'identité de la personne physique ou morale qui est le propriétaire du véhicule et l'identité du conducteur principal de ce dernier* ».

86. L'Autorité souligne que cette nouvelle obligation de conservation des données par les opérateurs constitue une ingérence dans le droit à la protection des données à caractère personnel qui, pour être admissible, doit poursuivre un objectif d'intérêt légitime et s'avérer nécessaire et proportionné à cet objectif. La justification avancée par le Gouvernement ne convainc pas l'Autorité de la nécessité et de la proportionnalité de la mesure. L'Autorité relève, par ailleurs, qu'il existe un risque que ces données soient utilisées à d'autres fins par les opérateurs. **Soit le Gouvernement est en mesure de montrer, à l'aide d'éléments factuels et concrets, qu'il est effectivement nécessaire et proportionné de conserver le numéro de châssis du véhicule dans lequel une de ses cartes SIM ou toute carte équivalente a été intégrée, ainsi que lien entre le numéro de châssis et le numéro de cette carte et cette justification doit se retrouver dans la justification de l'amendement proposée, soit le Gouvernement n'est pas en mesure d'apporter cette démonstration et cette disposition sera supprimée.**

E. Concernant l'amendement n° 7

87. L'amendement n° 7, qui entend insérer un **nouvel article 127/4** dans la loi télécom pour y reprendre une interdiction qui était auparavant inscrite à l'article 127 § 2 de la loi télécom, prévoit une interdiction de fournir ou d'utiliser un service ou un équipement qui empêche la réalisation des opérations suivantes :

1° les communications d'urgence, en ce compris l'identification de la ligne appelante et la fourniture des données d'identification de l'appelant ;
2° l'identification de l'utilisateur final, le repérage et la localisation des communications privées aux conditions prévues par la loi ;
3° les écoutes, la prise de connaissance et l'enregistrement des communications privées aux conditions prévues par le Code d'instruction criminelle et par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

88. **Comme l'Autorité l'a déjà relevé au considérant 162 de son avis n° 108/2021**, l'interdiction d'utiliser des systèmes qui peuvent empêcher l'identification de l'utilisateur final, le repérage et la localisation des communications non accessibles au public ainsi que la conservation des données d'identification, de trafic ou de localisation aboutit à rendre illégaux des services comme Tor, cmix et nym qui visent à permettre une utilisation anonyme du réseau Internet[54]. Une telle interdiction générale **constitue une ingérence disproportionnée dans le droit au respect de la vie privée des personnes concernées et qui excède dès lors ce qui est nécessaire dans une société démocratique**. Cette interdiction sera supprimée.

F. Concernant l'amendement n° 12

89. L'amendement n° 12 entend déterminer **les conditions auxquelles l'IBPT** peut accéder :

- aux « *données relatives à l'abonné ou à l'utilisateur habituel du service* », c'est-à-dire les données qui permettent d'établir l'identité civile de l'abonné qui est une personne physique ou de l'utilisateur habituel du service ou l'identité de l'abonné qui est une personne morale (nouvel article 15 § 1 de la loi IBPT).

- aux « *métadonnées de communications électroniques, autres que les données relatives à l'abonné ou à l'utilisateur habituel du service* », c'est-à-dire les données de trafic et de localisation autres que celles qui permettent d'identifier l'abonné ou l'utilisateur habituel du service (nouvel article 15 § 2 de la loi IBPT).

- aux bases de données des opérateurs mettant en œuvre les articles 122 à 127 de la loi télécom, à des fins de contrôle du respect de ces articles et de leurs arrêtés d'exécution (nouvel article 15 § 3 de la loi IBPT).

[54] L'Autorité relève que Tor, s'il peut effectivement être utilisé par des personnes qui souhaitent commettre des infractions, est également utilisé par des personnes qui défendent les droits fondamentaux, par des journalistes, par des organisations de la société civile et même par des services gouvernementaux (police, renseignements, …). La liste des sponsors de Tor révèle d'ailleurs bien que ce réseau n'est pas qu'un « repère de criminels » et qu'il présente au contraire une utilité pour des organisations de la société civile et des services gouvernementaux (voyez https://www.torproject.org/about/sponsors).

90. L'Autorité rappelle que, **dans son avis n° 32/2022** (voyez, en particulier, les considérants n° 58 et suivants), elle s'est prononcée sur certains aspects d'une disposition similaire à celle qui est examinée dans le cadre du présent avis. **L'Autorité y renvoie pour les aspects qui ne sont pas couverts par le présent avis**.

1. Quant à la nécessité pour l'IBPT d'avoir accès aux données d'identification des abonnés et utilisateurs habituels des services de communications électroniques et des métadonnées de communications

91. Le nouvel article 15 §§ 1 et 2 de la loi IBPT déterminent les finalités pour lesquelles l'IBPT peut accéder aux données conservées par les opérateurs. Il s'agit d'appliquer et de contrôler les dispositions énumérées à l'article 14, § 1er, 3°, a) et g) à i) de la loi IBPT, à savoir :
- la loi du 13 juin 2005 relative aux communications électroniques ;
- la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques, pour ce qui concerne les secteurs des communications électroniques et des infrastructures numériques ;
- la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, en ce qui concerne le secteur des infrastructures numériques ;
- le Règlement (UE) 611/2013 de la Commission du 24 juin 2013 concernant les mesures relatives à la notification des violations de données à caractère personnel en vertu de la Directive 2002/58/CE du Parlement européen et du Conseil sur la vie privée et les communications électroniques.

92. Comme l'Autorité l'a déjà relevé dans son avis n° 32/2022, **il appartient au législateur de s'assurer qu'il est effectivement nécessaire que l'IBPT ait accès aux données permettant d'identifier l'abonné ou l'utilisateur habituel du service et les métadonnées brutes de communications** en vérifiant, notamment, que l'IBPT n'est pas en mesure de remplir ses missions s'il n'a pas accès aux métadonnées de communications. L'Autorité souligne, en particulier, que **s'il est possible que l'IBPT remplisse toutes ou certaines des missions énumérées ci-dessus à l'aide de données anonymisées ou pseudonymisées**, le projet doit prévoir que seules des données anonymisées ou pseudonymisées pourront leur être transmises[55]. **Cet examen doit être fait de manière**

[55] L'Autorité souligne toutefois qu'il peut être particulièrement difficile de réellement anonymiser ou même pseudonymiser des métadonnées de communications électroniques. Il apparait, en effet, qu'il est tout à fait possible voire assez facile, de réidentifier des personnes à partir d'un set de métadonnées de communications électroniques anonymisées. Voir Ana-Maria Creţu, Federico Monti, Stefano Marrone, Xiaowen Dong, Michael Bronstein, Yves-Alexandre de Montjoye, "Interaction data are identifiable even across longperiods of time", *Nature Communications*, 25 janvier 2022

minutieuse, mission par mission. La justification de l'amendement ne démontre pas que le Gouvernement a effectivement réalisé cet examen.

93. Comme dans son avis n° 32/2022, l'Autorité rappelle que, **si et dans la mesure où l'IBPT a pour mission de service publique de détecter, en temps réel, des cyberattaques et d'y mettre fin** (ce qui peut impliquer de devoir bloquer certains services ou certaines adresses IP afin de mettre fin, par exemple, à des attaques DDOS, de désactiver des botnets ou encore de mettre fin à des tentatives de phishing), **l'Autorité comprend que l'IBPT doit pouvoir accéder à des métadonnées brutes de communications électroniques**. Toutefois, au vu de la gravité de l'ingérence qu'un tel accès cause dans le droit au respect de la vie privée, l'Autorité considère **qu'il est essentiel de tenir un débat parlementaire approfondi afin de définir les contours exacts des pouvoirs et des missions** des services de police, des services judiciaires, des services de renseignements, des services militaires ou encore des autorités administratives chargées de détecter et de lutter contre les cyberattaques. L'Autorité **insiste pour que ce débat porte aussi sur les nécessaires limites à mettre en place** concernant les traitements ultérieurs des métadonnées (par exemple par les services de renseignements ou les services de police) qui auront été collectées dans le cadre de la lutte contre cybercriminalité.

2. Quant à l'accès de l'IBPT aux données d'identifications des abonnés et utilisateurs habituels

94. Le **nouvel article 15 § 1er** de la loi IBPT porte sur l'accès « *aux données relatives à l'abonné ou à l'utilisateur habituel du service* » lorsque cela s'avère nécessaire pour accomplir l'une des missions de l'IBPT qu'il liste. L'IBPT peut formuler une demande écrite et motivée directement à l'opérateur qui est tenu de lui répondre. Le nouvel article 15 § 5 précise que la motivation doit porter sur le lien entre les données demandées et la mission de l'IBPT et le caractère strictement nécessaire des données demandées dans le cadre de la mission. Aucun contrôle préalable n'est prévu.

95. **Sous réserve qu'il soit effectivement nécessaire que l'IBPT ait effectivement accès** aux données d'identification des abonnés ou des utilisateurs habituels des services de communications électroniques pour l'exercice de (certaines de) ses missions – ce qu'il appartient au législateur de vérifier –, **les modalités de cet accès** aux données d'identification des abonnés ou des utilisateurs habituels des services de communications électroniques **sont conformes aux exigences énoncées par la Cour constitutionnelle dans son arrêt n° 158/2021.** L'Autorité **en prend donc note**.

3. Quant à l'accès de l'IBPT aux métadonnées des communications électroniques

96. Le nouvel article 15 § 2 porte sur l'accès aux « *métadonnées de communications électroniques, autres que les données relatives à l'abonné ou à l'utilisateur habituel du service* ». **L'accès à ces données** est subordonné, sauf cas d'urgence dûment motivée, à **l'autorisation écrite préalable de l'Autorité**, qui se voit donc confier une nouvelle mission.

3.1. Quant aux catégories de métadonnées auxquelles l'IBPT peut avoir accès

97. L'Autorité constate, tout d'abord, qu'il n'y **pas de précision concernant les métadonnées** de communications électroniques **auxquelles l'IBPT peut accéder**. La disposition en projet est formulée de manière très large et permet *a priori* à l'IBPT de demander un accès à toutes les données conservées par les opérateurs, y compris les données conservées en exécution du nouvel article 126/1 de la loi télécom qui – pour rappel – impose aux opérateurs de conserver, en principe, **pendant 12 mois**[56], les **données de trafic et de localisation** de **toutes les communications** effectuées **à partir**, ou **vers**, une des **zones géographiques** qu'il liste. Or, au **vu de l'ingérence particulièrement grave** causée par la conservation de données prévue par le nouvel article 126/1 de la loi télécom, le principe de proportionnalité, tel qu'il a été interprété par la CJUE, exige que l'accès à ces données ne puisse être prévu qu'afin de poursuivre l'un des objectifs listés à l'article 15 de la directive ePrivacy qui présente un degré d'importance particulièrement élevé. **L'Autorité constate que l'auteur de l'amendement n'apporte aucune justification quant au fait que les missions remplies par l'IBPT (pour lesquelles l'IBPT peut solliciter un accès aux métadonnées de communications) présentent une importance telle que cela peut justifier une ingérence particulièrement grave dans les droits et libertés des personnes concernées**.

98. **À défaut d'une justification étayée de l'importance de l'objectif poursuivi** (à la lumière des exigences mises en évidence par la CJUE), **la disposition en projet devra être modifiée afin d'exclure la possibilité pour l'IBPT de demander accès à aux données conservées en exécution de l'article 126/1 de la loi télécom**.

99. Par ailleurs, et plus généralement, l'Autorité relève que l'exigence de prévisibilité, couplée au principe de minimisation des données consacré par l'article 5.1. c) du RGPD, requiert que la disposition en projet **délimite précisément quelles sont les catégories de données auxquelles l'IBPT peut avoir accès pour remplir quelles missions**. En d'autres termes, la disposition en projet doit identifier, pour chaque mission de l'IBPT, les catégories de données auxquelles cette institution doit avoir accès pour remplir les missions de service public qui leur sont confiées, étant donné que ces

[56] A moins qu'une autre durée soit prévue par ce nouvel article 126/1 de la loi télécom. Cette disposition prévoit des durées de conservation plus courtes dans certaines circonstances. Voyez le nouvel article 126/1 § 3, 1° de la loi télécom.

catégories de données doivent être « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées* ».

3.2. Quant aux modalités du contrôle préalable à l'accès des métadonnées par l'IBPT

100. Dans son avis **n° 32/2022,** l'Autorité s'est déjà prononcée **sur les modalités du contrôle préalable** envisagé pour l'accès aux métadonnées de communications électroniques par l'IBPT.

101. L'Autorité a également émis, **dans l'annexe de l'avis concernant un avant-projet de loi modifiant la loi portant création de l'APD[57],** des considérations détaillées à propos **de la nouvelle compétence d'autorisation préalable** qui lui serait attribuée.

102. **L'Autorité y renvoie et insiste pour que les observations émises aux considérants 66 à 73 de l'avis n° 32/2022 et aux considérants 59 à 64 de l'annexe à l'avis sur l'avant-projet de loi modifiant la loi portant création de l'APD, soient dûment prises en compte**.

4. Quant aux modalités de consultation des bases de données qui mettent en œuvre les articles 122, 123, 126, 126/1, 126/2 et 127 de la loi télécom

103. Le nouvel article 15 § 3 de la loi IBPT vise la situation spécifique dans laquelle l'IBPT agit comme autorité de contrôle des dispositions nationales prises en application de la directive ePrivacy. La disposition en projet prévoit que les modalités auxquelles l'IBPT peut consulter les bases de données mettant en œuvre les articles 122, 123, 126, 126/1, 126/2 et 127 de la loi télécom, et ce afin de contrôler le respect, par un opérateur, de ces dispositions. L'**Autorité prend note de ces modalités qui n'appelle pas de commentaire de sa part**.

G. Concernant l'amendement n° 15

104. L'amendement n° 15 vise à insérer **un nouvel article 25/1 dans la loi IBPT**.

105. Le nouvel **article 25/1 § 1er** de la loi IBPT entend autoriser un officier de police judiciaire de l'IBPT d'exiger, sur base de demande écrite et motivée, des informations lui permettant **d'identifier l'abonné ou l'utilisateur habituel** d'un service de communications électroniques, et ce afin **de rechercher, de constater ou de poursuivre une infraction** visée à l'article 145, § 3 ou § 3bis, de la loi télécom ou à l'article 24, § 1er , 2° de la loi IBPT.

[57] Disponible ici : https://www.autoriteprotectiondonnees.be/publications/annexe-avis-sur-lavant-projet-de-loi-portant-modification-de-la-loi-apd.pdf

106. Pour procéder à cette identification, l'officier de police judiciaire peut exiger de l'opérateur qu'il lui fournisse les données relatives à l'abonné ou à l'utilisateur habituel du service qui sont nécessaire à cette fin. L'officier de police judiciaire peut également requérir la collaboration :
(1) des banques et institutions financières (au cas où les opérateurs communiquent la référence d'une transaction bancaire électronique),
(2) des centres fermés et lieux d'hébergement pour étrangers (au cas où la souscription de l'abonné à un service de communications électroniques a été effectué, sur la base des coordonnées du centre ou du lieu d'hébergement qui ont préalablement été communiquées par un opérateur), ou
(3) de toute autre personne morale qui est l'abonné d'un opérateur ou qui souscrit à un service de communications électroniques au nom et pour le compte de personnes physiques, sur la base des données qui ont préalablement été communiquées par un opérateur.

107. Le nouvel article 25/1 § 5 précise que la motivation de la demande d'identification doit porter sur (1) le lien entre les données demandées et l'objectif de recherche, de constat ou de poursuite de l'infraction spécifique qui justifie la demande et sur (2) le caractère strictement nécessaire des données demandées dans le cadre de l'enquête. Aucun contrôle préalable n'est prévu.

108. À propos du pouvoir de l'officier de police judiciaire d'identifier les abonnés et les utilisateurs habituels d'un service de communications électroniques, **l'Autorité renvoie aux observations qu'elle a émises ci-dessus** concernant **l'extension de l'obligation d'identification** et **la mise en place des méthodes d'identification indirecte**.

109. Concernant les modalités d'accès à ces informations (exigence en termes de motivation de la demande et absence de contrôle préalable), l'Autorité constate qu'elles **sont conformes aux exigences énoncées par la Cour constitutionnelle dans son arrêt n° 158/2021.** L'Autorité **en prend donc note**.

110. Le nouvel **article 25/1 § 2** de la loi IBPT entend autoriser un officier de police judiciaire de l'IBPT d'exiger, en principe après autorisation d'un juge d'instruction, d'un opérateur de lui fournir **les métadonnées de communications électroniques** qui sont nécessaires afin **de rechercher, de constater ou de poursuivre une infraction** visée à l'article 145, § 3 ou § 3bis, de la loi télécom ou à l'article 24, § 1er , 2° de la loi IBPT.

111. L'Autorité constate qu'il n'y **pas de précision concernant les métadonnées** de communications électroniques **auxquelles l'officier de police judiciaire de l'IBPT peut accéder**. La disposition en projet est formulée de manière très large et permet *a priori* de demander un accès à toutes les données conservées par les opérateurs, y compris les données conservées en exécution du nouvel

article 126/1 de la loi télécom. Or, au **vu de l'ingérence particulièrement grave** causée par la conservation de données prévue par le nouvel article 126/1 de la loi télécom, le principe de proportionnalité, tel qu'il a été interprété par la CJUE, exige que l'accès à ces données ne puisse être prévu qu'afin de lutter contre la criminalité grave. **L'Autorité constate que l'auteur de l'amendement n'apporte aucune justification quant au fait que les infractions recherchées et poursuivies par les officiers de police judiciaire de l'IBPT (pour lesquelles ils peuvent solliciter un accès aux métadonnées de communications) relèvent de la criminalité grave**.

112. **À défaut d'une justification étayée de l'importance de l'objectif poursuivi** (à la lumière des exigences mises en évidence par la CJUE), **la disposition en projet devra être modifiée afin d'exclure la possibilité pour l'IBPT de demander accès à aux données conservées en exécution de l'article 126/1 de la loi télécom**.

113. Pour le surplus, l'Autorité constate que **les modalités prévues pour l'accès à ces données** (exigence en termes de motivation et existence d'un contrôle préalable) **sont conformes aux exigences imposées par la CJUE**.

114. Le **nouvel 25/1 § 3** de la loi IBPT entend autoriser un officier de police judiciaire de l'IBPT de **consulter les bases de données** qui mettent en œuvre les articles 126, 126/1, 126/2 et 127 de la loi télécom, et **ce afin de contrôler le respect de ces dispositions** dont la violation est sanctionnée pénalement. L'Autorité n'a **pas de remarque à formuler** à propos de cette disposition.

H. Concernant les amendements n° 16 à 18

115. **L'amendement n° 16** entend modifier l'article 46bis du C.I.C afin de permettre au Procureur du Roi, pour procéder à l'identification de l'abonné ou de l'utilisateur habituel d'un service de communications électroniques, de requérir directement ou par l'intermédiaire du service de police désigné par le Roi, la collaboration :

(1) Des banques et des établissements financiers sur la base de la référence d'une transaction bancaire électronique qui lui a été préalablement communiquée par un opérateur (identification par le bais d'une méthode indirecte)

(2) Des centres fermés et autres lieux d'hébergements pour étrangers sur la base des coordonnées du centre ou du lieu d'hébergement où la souscription de l'abonné à un service de communications électroniques mobiles a été effectué, et qui ont préalablement été communiquées par un opérateur (identification par le bais d'une méthode indirecte)

(3) Des autres personnes morales qui sont l'abonné d'un opérateur, ou qui souscrivent à un service de communications électroniques au nom et pour le compte de personnes physiques, sur la base

des données qui lui ont préalablement été communiquées par un opérateur (identification par le bais d'une méthode indirecte).

116. L'article 46bis du C.I.C est modifié afin d'y prévoir explicitement le pouvoir du Procureur du Roi d'identifier l'abonné ou l'utilisateur habituel d'un service de communications électroniques par le biais d'une méthode d'identification indirecte conformément à ce que permet le nouvel article 127 de la loi télécom (qui est introduit par l'amendement n° 6). À ce propos, **l'Autorité renvoie aux observations qu'elle a émises ci-dessus** concernant **l'extension de l'obligation d'identification** et **la mise en place des méthodes d'identification indirecte**.

117. **L'amendement n° 17** entend compléter l'article 11 § 1er de la loi du 24 janvier 1977 afin de permettre au chef du service Inspection produits de consommation (du SPF Santé publique, Sécurité de la chaîne alimentaire et Environnement) de requérir la collaboration des banques et des établissements financiers « *sur la base de la référence d'une transaction bancaire électronique qui a préalablement été communiquée* ».

118. Il **ne** ressort **pas** de la disposition en projet, telle qu'elle sera insérée à la fin de l'article 11 § 1er de la loi du 24 janvier 1977, que **la référence de la transaction bancaire** électronique doit avoir été communiquée au chef du service Inspection produits de consommation **par un opérateur télécom**. Or une telle précision, qui circonscrit le pouvoir de l'administration, est essentielle tant pour assurer la prévisibilité que la proportionnalité de l'ingérence dans le droit à la protection des données à caractère personnel. **L'amendement sera modifié afin d'y inclure cette précision**. Pour le surplus, l'Autorité **renvoie aux observations** qu'elle a émises ci-dessus **concernant l'extension de l'obligation d'identification** et la **mise en place d'une méthode d'identification indirecte** à partir de la référence d'une transaction bancaire électronique.

119. **L'amendement n° 18** entend modifier l'article 81 de la loi du 2 août 2002 afin de permettre à l'auditeur de la FSMA (ou l'auditeur adjoint en cas d'absence de ce dernier), pour procéder à l'identification de l'abonné ou de l'utilisateur habituel d'un service de communications électroniques, de requérir la collaboration :
    (1) Des banques et des établissements financiers sur la base de la référence d'une transaction bancaire électronique qui lui a été préalablement communiquée par un opérateur (identification par le bais d'une méthode indirecte)
    (2) Des centres fermés et autres lieux d'hébergements pour étrangers sur la base des coordonnées du centre ou du lieu d'hébergement où la souscription de l'abonné à un service

de communications électroniques mobiles a été effectué, et qui ont préalablement été communiquées par un opérateur (identification par le bais d'une méthode indirecte)

(3) Des autres personnes morales qui sont l'abonné d'un opérateur, ou qui souscrivent à un service de communications électroniques au nom et pour le compte de personnes physiques, sur la base des données qui lui ont préalablement été communiquées par un opérateur (identification par le bais d'une méthode indirecte).

120. L'Autorité **renvoie aux observations** qu'elle a émises ci-dessus **concernant l'extension de l'obligation d'identification et la mise en place des méthodes d'identification indirecte**.

PAR CES MOTIFS :

L'Autorité attire l'attention du Gouvernement et des parlementaires sur les éléments suivants :

- Il convient de s'assurer que le projet de loi de réparation de la loi *data retention* a été revu en profondeur pour répondre aux remarques et observations fondamentales soulevées par l'Autorité dans son avis n° 108/2021. Le législateur doit veiller, en particulier, à ce que le projet de loi de réparation n'impose pas, *de jure ou de facto*, des obligations de conservation préventive des données de trafic ou de localisation de l'ensemble ou d'une proportion trop importante des utilisateurs de moyens de communications électroniques en Belgique, à moins qu'il existe des circonstances suffisamment concrètes permettant de considérer que l'État fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible (cons. 20 ; cons. 32)

- Les nouvelles définitions des notions d'« opérateur » et de « services de communications électroniques », couplées, notamment, à l'obligation d'identification imposée par les nouveaux articles 126 et 127 de la loi télécom, aboutissent à rendre impossible – ou en tout cas très difficile – toute correspondance anonyme sur Internet. Ceci constitue un changement de paradigme par rapport au paradigme de, et aux règles de confidentialité imposées par, la directive ePrivacy. Il convient de tenir un débat parlementaire approfondi sur les implications de ce changement, notamment, au regard du droit à la vie privée et du droit à la liberté d'expression (cons. 23-24 ; 40-41).

- L'identification de l'abonné à un service de communications électroniques ne permet pas nécessairement d'identifier l'utilisateur effectif de ce service (cons. 42 ; 73). Au vu de ce constat et de la difficulté de rapporter une preuve négative, l'Autorité invite les parlementaires à être très prudents avant de maintenir et d'étendre les conditions d'application d'une présomption réfragable selon

laquelle « *la personne identifiée est présumée utiliser elle-même le service de communications électronique*s » (cons. 78)

- Lorsque le Roi autorisera des méthodes identification spécifiques, le cas échéant indirectes, pour les personnes qui ne disposent d'aucun des documents d'identité, listés dans le nouvel article 127 de la loi télécom, le Roi devra veiller au respect des principes de nécessité et de proportionnalité (cons. 67)

- Les amendements visent à étendre les catégories d'autorités qui peuvent identifier les abonnés et utilisateurs finaux des services de communications électroniques, y compris par le biais de méthodes d'identification indirectes. Les parlementaires doivent s'assurer que cette extension (et l'aggravation de l'ingérence qu'elle cause dans les droits et libertés des personnes concernées) est bien nécessaire et proportionné à l'objectif poursuivi, étant donné que la justification de la nécessité et de la proportionnalité doit reposer sur des éléments factuels et concrets (cons. 74, 108 ; 116; 120)

- Il appartient au législateur de s'assurer qu'il est effectivement nécessaire que l'IBPT ait accès aux données permettant d'identifier l'abonné ou l'utilisateur habituel du service et les métadonnées brutes de communications en vérifiant, notamment, que l'IBPT n'est pas en mesure de remplir ses missions s'il n'a pas accès aux métadonnées de communications. L'Autorité souligne, en particulier, que s'il est possible que l'IBPT remplisse toutes ou certaines des missions énumérées ci-dessus à l'aide de données anonymisées ou pseudonymisées, le projet doit prévoir que seules des données anonymisées ou pseudonymisées pourront leur être transmises (cons. 92). Si et dans la mesure où l'IBPT a pour mission de service publique de détecter, en temps réel, des cyberattaques et d'y mettre fin (ce qui peut impliquer de devoir bloquer certains services ou certaines adresses IP afin de mettre fin, par exemple, à des attaques DDOS, de désactiver des botnets ou encore de mettre fin à des tentatives de phishing), l'Autorité comprend que l'IBPT doit pouvoir accéder à des métadonnées brutes de communications électroniques. Toutefois, au vu de la gravité de l'ingérence qu'un tel accès cause dans le droit au respect de la vie privée, l'Autorité considère qu'il est essentiel de tenir un débat parlementaire approfondi afin de définir les contours exacts des pouvoirs et des missions des services de police, des services judiciaires, des services de renseignements, des services militaires ou encore des autorités administratives chargées de détecter et de lutter contre les cyberattaques (cons. 93)

- Concernant la nouvelle compétence d'autorisation que les amendements entendent confier à l'Autorité, l'Autorité renvoie et insiste pour que les observations émises aux considérants 66 à 73 de l'avis

n° 32/2022 et aux considérants 59 à 64 de l'annexe à l'avis sur l'avant-projet de loi modifiant la loi portant création de l'APD, soient dûment prises en compte (con. 100-102)

L'Autorité estime que les modifications suivantes doivent être apportées aux amendements :

- Supprimer le nouvel article 126/2 § 1er, 9° et 10° (ou du moins celles pour lesquelles l'auteur n'est en mesure d'en justifier la conservation), à moins que l'auteur de l'amendement soit en mesure de montrer, à l'aide d'éléments factuels et concrets, en quoi la conservation de ces catégories de données est nécessaire et proportionnée au regard de l'objectif poursuivi, et cette explication est ajoutée dans la justification de l'amendement (cons. 35)

- Supprimer le nouvel article 126/2 § 1er, 11° (cons. 36)

- Imposer aux points de vente de services de communications électroniques d'introduire directement dans les systèmes informatiques de l'opérateur les données d'identification de l'abonné et leur interdire toute prise de copie de document d'identité (cons. 46).

- Supprimer la possibilité offerte aux opérateurs et canaux de vente de services de communications électroniques de recourir à une méthode automatique de comparaison entre les paramètres biométriques sur la photo du document d'identité de l'abonné et ceux de son visage (cons. 49-53)

- Dans le nouvel article 127 § 4, dernier alinéa, de la loi télécom, supprimer les mots « *et que l'opérateur n'a pas mis en œuvre la méthode de comparaison faciale visée à l'alinéa 3* » et de remplacer le mot « *peut* » par le mot « *doit* » (cons. 55)

- Supprimer le nouvel article 127 § 5, alinéa 3 et prévoir uniquement la mention, dans la base de données établie par les opérateurs en vertu de l'article 127 de la loi télécom, des données d'identité collectées à partir de la consultation des documents d'identité (cons. 57) et, pour une identité de motifs, supprimer, dans le nouvel article 127, § 10, alinéa 2, l'obligation consiste à fournir « *à l'opérateur une copie du document d'identification des abonnés, sauf lorsqu'il s'agit de la carte d'identité électronique belge, conformément au paragraphe 5, alinéa 3* » (cons. 82)

- Suppression du nouvel article 127 § 5, alinéas 4 et 5 (cons. 58-66)

- Fixer une liste unique des données d'identification à conserver, quitte à préciser que certaines données ne doivent être conservées que dans la mesure où elles existent pour la personne concernée (cons. 68-69)

- Supprimer « *la photo de l'abonné mais uniquement pour les documents d'identité autres que la carte d'identité électronique belge* » de la liste maximale des données qui peuvent/doivent être conservées (cons. 70, a))

- Supprimer l'adresse du domicile, l'adresse email et le numéro de téléphone de la liste des données d'identification que les opérateurs doivent conserver (cons. 70, b))

- Définir le « *numéro de sécurité publique* », éventuellement par un renvoi à la règlementation définissant déjà cette notion (cons. 70, c))

- Préciser que le numéro du document d'identité ne peut être conservé que dans la situation où l'opérateur ne dispose pas déjà du numéro de registre national (cons. 70, d))

- Prévoir que, lorsque l'abonné est identifié à partir d'une carte d'identité électronique belge, l'opérateur ne peut conserver que le numéro de registre national, le nom et le prénom (cons. 70, e))

- Supprimer la délégation au Roi prévue par le nouvel article 127 § 6, alinéa 2 (cons. 70, f))

- Supprimer la date et le lieu de naissance de la liste des données à collecter dans le cadre de la méthode d'identification indirecte en cas de paiement électronique en ligne spécifique à la souscription d'un service de communications électroniques (cons. 76)

- Limiter la conservation des adresses IP ayant servi à la création du compte et des adresses IP attribuées à la source de la connexion à 12 mois après la fin de la session (cons. 77)

- Supprimer le nouvel article 127 § 10, alinéa 5, à moins que le Gouvernement soit en mesure de montrer, à l'aide d'éléments factuels et concrets, qu'il est effectivement nécessaire et proportionné de conserver le numéro de châssis du véhicule dans lequel une de ses cartes SIM ou toute carte équivalente a été intégrée, ainsi que lien entre le numéro de châssis et le numéro de cette carte (auquel cas la justification doit se retrouver dans la justification de l'amendement proposé) (cons. 86)

- Supprimer l'interdiction imposée par le nouvel article 127/4 de la loi télécom (cons. 88)

- Exclure la possibilité pour l'IBPT de demander accès aux données conservées en exécution de l'article 126/1 de la loi télécom (cons. 97-98 ; 111-112)

- Identifier, pour chaque mission de l'IBPT, les catégories de données auxquelles cette institution doit avoir accès pour remplir les missions de service public qui leur sont confiées (cons. 99)

- Revoir les modalités de contrôle préalable à l'accès aux métadonnées par l'IBPT conformément aux observations émises aux considérants 66 à 73 de l'avis de l'Autorité n° 33/2022 (cons. 100-102)

- Préciser, dans le dispositif de l'article 11 § 1er de la loi du 24 janvier 1977, que la référence de la transaction bancaire électronique doit avoir été communiquée au chef du service Inspection produits de consommation par un opérateur télécom (cons. 118)

Pour le Centre de Connaissances,
(sé) Rita Van Nuffelen – Responsable a.i. du Centre de Connaissances