Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 108/2021 du 28 juin 2021

Objet : Demande d'avis concernant un avant-projet de loi relatif à la collecte et à la conservation des données d'identification, de trafic et de localisation dans le secteur des communications électroniques et à leur accès par les autorités et un projet d'arrêté royal modifiant l'arrêté royal du 19 septembre 2013 portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques (CO-A-2021-099)

Le Centre de Connaissances de l'Autorité de protection des données (ci-après « l'Autorité »),
Présent.e.s : Madame Alexandra Jaspar et Messieurs Yves-Alexandre de Montjoye, Bart Preneel et Frank Robben ;

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 Ministre de la Justice, Monsieur Vincent Van Quickenborne, reçue le 7 mai 2021 ;

Vu les informations complémentaires transmises les 1er et 8 juin 2021 ;

Vu le rapport d'Alexandra Jaspar ;

Émet, le 28 juin 2021, l'avis suivant :

I. OBJET ET CONTEXTE DE LA DEMANDE D'AVIS

1. Le Ministre de la Justice, Monsieur Vincent Van Quickenborne (ci-après « le demandeur ») a sollicité, le 7 mai 2021, l'avis de l'Autorité concernant un avant-projet de loi relatif à la collecte et à la conservation des données d'identification, de trafic et de localisation dans le secteur des communications électroniques et à leur accès par les autorités (ci-après « l'avant-projet de loi ») et un projet d'arrêté royal modifiant l'arrêté royal du 19 septembre 2013 portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques (ci-après « le projet d'arrêté »).

2. L'avant-projet de loi vise, comme le souligne son Exposé des Motifs, *« à répondre 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 l'Exposé des motifs de l'avant-projet, « *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 et en particulier pour les enquêtes pénales* ». Cette loi imposait ainsi une obligation de conservation généralisée et indifférenciée de certaines données de trafic et de localisation. 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. L'avant-projet entend mettre en place un système de conservation des données de communication qui respecte les exigences imposées par la CJUE. Pour ce faire, il entend modifier la loi du 13 juin 2005 relative aux communications électroniques (ci-après « la loi télécom »), le Code d'instruction criminelle (ci-après « le CIC »), la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges (ci-après « la loi statut IBPT »), la loi du 5 août 1992 sur la fonction

[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.

de police (ci-après « la loi sur la fonction de police »), la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (ci-après « la loi sur les services de renseignement »), la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers (ci-après « la loi FSMA »), 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 relative à la protection de la santé des consommateurs ») et 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 (ci-après « la loi NIS »).

5. Le projet d'arrêté, pour sa part, exécute certaines habilitations législatives contenues dans l'avant-projet.

II. EXAMEN DE LA DEMANDE D'AVIS

6. Dans son avis, l'Autorité commence par identifier les dispositions de la Directive ePrivacy qui sont transposées par l'avant-projet de loi (A). Elle poursuit en présentant le « système » que l'avant-projet de loi entend mettre en place concernant la conservation des données de trafic et de localisation par les opérateurs et leur accès par différentes autorités (B). L'Autorité rappelle, ensuite, les exigences auxquelles doivent répondre les normes qui prévoient une conservation des données de trafic et/ou de localisation (et leur communication éventuelle aux autorités) (C). Enfin, l'Autorité examine la conformité de l'avant-projet de loi et du projet d'arrêté avec ces exigences (D).

7. À toutes fins utiles, l'Autorité souligne qu'elle se prononce uniquement sur les dispositions pour lesquelles elle est compétente, à l'exclusion des dispositions qui relèvent de la compétence exclusive d'une autre autorité de contrôle. Pour rappel, c'est l'Organe de contrôle de l'information policière (ci-après « le COC ») qui est compétent pour l'examen des dispositions prévoyant des traitements de données à caractère personnel effectués par la police intégrée et c'est le Comité permanent de contrôle des services de renseignement et de sécurité (ci-après « le Comité R ») qui est compétent pour l'examen des dispositions qui prévoient des traitements de données effectués par les services de renseignement et de sécurité.

A. LES DISPOSITIONS PERTINENTES DE LA DIRECTIVE ePRIVACY

8. La directive ePrivacy, qui précise et complète le RGPD en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques, entend protéger les utilisateurs des services de communications électroniques contre les dangers pour leurs données à caractère personnel et leur vie privée résultant des nouvelles technologies.

9. L'avant-projet de loi transpose certaines dispositions de cette directive, et en particulier ses articles 5, 6, 9 et 15. À des fins de lisibilité et de clarté, l'Autorité reprend ces dispositions ci-dessous.

10. **L'article 5.1 de la Directive ePrivacy** impose aux Etats de garantir « *la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, paragraphe 1. Le présent paragraphe n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité* »[2].

11. **L'article 6.1 de la Directive ePrivacy rappelle et précise la portée du principe de la confidentialité des données relatives au trafic** : « *Les données relatives au trafic concernant les abonnés et les utilisateurs traitées et stockées par le fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessibles au public doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication sans préjudice des paragraphes 2, 3 et 5, du présent article ainsi que de l'article 15, paragraphe 1* »[3].

12. **L'article 6.2 de la Directive ePrivacy** autorise le traitement des données relatives au trafic « *qui sont nécessaires pour établir les factures des abonnés et les paiements pour interconnexion. Un tel traitement n'est autorisé que jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement* »[4].

13. **L'article 6.3 de la Directive ePrivacy** autorise le fournisseur d'un service de communications électronique accessible au public à traiter les données relatives au trafic « *dans la mesure et pour la durée nécessaires à la fourniture ou à la commercialisation de [de services de communications électroniques ou de fournir des services à valeur ajouté], pour autant que l'abonné ou l'utilisateur que concernent ces données ait donné son consentement préalable. Les utilisateurs ou abonnés ont la possibilité de retirer à tout moment leur consentement pour le traitement des données relatives au trafic* »[5].

14. **L'article 6.5 de la Directive ePrivacy** dispose que *« Le traitement des données relatives au trafic effectué conformément aux dispositions des paragraphes 1, 2, 3 et 4 doit être restreint aux personnes*

[2] C'est l'Autorité qui souligne
[3] C'est l'Autorité qui souligne.
[4] C'est l'Autorité qui souligne.
[5] C'est l'Autorité qui souligne.

agissant sous l'autorité des fournisseurs de réseaux publics de communications et de services de communications électroniques accessibles au public qui sont chargées d'assurer la facturation ou la gestion du trafic, de répondre aux demandes de la clientèle, de détecter les fraudes et de commercialiser les services de communications électroniques ou de fournir un service à valeur ajoutée; ce traitement doit se limiter à ce qui est nécessaire à de telles activités » alors que **l'article 6.6 de cette même Directive** indique que « *Les paragraphes 1, 2, 3 et 5 s'appliquent sans préjudice de la possibilité qu'ont les organes compétents de se faire communiquer des données relatives au trafic conformément à la législation en vigueur dans le but de régler des litiges, notamment en matière d'interconnexion ou de facturation* ».

15. **L'article 9.1 de la Directive ePrivacy** dispose que « *Lorsque des données de localisation, autres que des données relatives au trafic, concernant des utilisateurs ou abonnés de réseaux publics de communications ou de services de communications électroniques accessibles au public ou des abonnés à ces réseaux ou services, peuvent être traitées, elles ne le seront qu'après avoir été rendues anonymes ou, moyennant le consentement des utilisateurs ou des abonnés, dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée. […]* »[6].

16. Aux termes de **l'article 9.3 de la Directive ePrivacy**, « *Le traitement des données de localisation autres que les données relatives au trafic effectué conformément aux paragraphes 1 et 2 doit être restreint aux personnes agissant sous l'autorité du fournisseur du réseau public de communications ou service de communications électroniques accessible au public ou du tiers qui fournit le service à valeur ajoutée, et doit se limiter à ce qui est nécessaire pour assurer la fourniture du service à valeur ajoutée* ».

17. **L'article 15.1 de la Directive ePrivacy** se lit comme suit : « *Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, […] et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale — c'est-à-dire la sûreté de l'État — la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent*

[6] C'est l'Autorité qui souligne.

paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne »[7].

B. PRESENTATION DU « SYSTEME » PROPOSE PAR L'AVANT-PROJET DE LOI CONCERNANT LA CONSERVATION DES DONNEES DE COMMUNICATION PAR LES OPERATEURS TELECOM ET LEURS COMMUNICATIONS EVENTUELLES AUX AUTORITES[8]

❖ *Quant aux données qui peuvent ou doivent être conservées par les opérateurs*

18. Plusieurs dispositions de la loi télécom, que l'avant-projet de loi prévoit de modifier, permettent ou imposent la conservation, par les opérateurs, des données de trafic et/ou de localisation (y compris des données de localisation autres que des données de trafic), et ce pour différentes finalités :

    1) Les opérateurs **peuvent** conserver et traiter **les données de trafic nécessaires à l'établissement des factures des abonnés** ou **celles qui sont nécessaires aux paiements d'interconnexion** (**nouvel article 122 § 2** de la loi télécom[9])[10].

    Ces données peuvent être conservées *« **jusqu'à la fin de la période de contestation de la facture ou jusqu'à la fin de la période au cours de laquelle une action peut être menée pour en obtenir le paiement** »* (nouvel article 122 § 2, dernier alinéa, de la loi télécom).

    La loi télécom donne uniquement une **définition fonctionnelle des données qui peuvent être conservées** : les données de trafic nécessaires à l'établissement de la facture de l'abonné ou au paiement d'interconnexion. Au contraire de ce qui est prévu dans la version actuelle de l'article 122 § 2 de la loi télécom, la nouvelle version de cette

[7] C'est l'Autorité qui souligne. L'article 6 §§ 1 et 2 du traité sur l'Union européenne se lit comme suit : « *1. L'Union reconnaît les droits, les libertés et les principes énoncés dans la Charte des droits fondamentaux de l'Union européenne du 7 décembre 2000, telle qu'adaptée le 12 décembre 2007 à Strasbourg, laquelle a la même valeur juridique que les traités […].*
2. L'Union adhère à la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales […] ».
[8] L'Autorité a synthétisé ce système dans un tableau repris dans l'Annexe II.
[9] L'article 122 § 2 de la loi télécom transpose l'article 6 § 2 de la Directive ePrivacy.
[10] La version actuelle de l'article 122 § 2 de la loi télécom impose – au lieu d'autoriser – aux opérateurs de conserver des données de trafic dans le but d'établir les factures des abonnés ou d'effectuer les paiements d'interconnexion. Cet article prévoira à l'avenir uniquement une possibilité pour les opérateurs. Le passage d'une obligation de conservation vers une possibilité est justifiée comme suit dans l'Exposé des motifs : *« D'une part, une obligation n'est pas nécessaire, étant donné que les opérateurs ont tout intérêt à conserver ces données pour ces finalités et qu'il découle de l'article 110 de la [loi télécom], à tout le moins indirectement, que ces données doivent être disponibles [l'article 110 de la loi télécom impose aux opérateurs de fournir une facture détaillée de base aux abonnés et permet aux abonnés d'obtenir gratuitement, sur simple demande, une version plus détaillée de la facture de base qu'ils ont reçue]. D'autre part, cette modification permet de se rapprocher de l'article 6, § 2, de la directive [ePrivacy] que l'article 122, § 2 transpose. Cet article 6, § 2, prévoit que, par dérogation au principe de suppression ou d'anonymisation, les données de trafic peuvent être traitées à des fins de facturation* »

disposition ne détermine plus les catégories de données de trafic précises qui peuvent être conservées à cette fin[11].

2) Les opérateurs **peuvent traiter des données de trafic nécessaires** afin (i) d'assurer le **marketing des services de communications électroniques propres** et (ii) **d'établir le profil d'utilisation de l'abonné** ou de l'utilisateur final[12], **à condition d'avoir obtenu le consentement** de l'abonné ou, le cas échéant, de l'utilisateur final (**nouvel article 122 § 3** de la loi télécom)[13]

3) Les opérateurs **doivent conserver** des **données de localisation et d'autres des données de trafic nécessaires** afin de **détecter et d'analyser une fraude présumée[14]** ou **une utilisation malveillante présumée[15]** du réseau de communications électroniques (**nouvel article 122 § 4** de la loi télécom).

Cette disposition prévoit que **les données de localisation et les autres données de trafic nécessaires** afin de détecter et d'analyser une fraude présumée ou une utilisation malveillante présumée du réseau de communications électroniques **doivent être conservées pour minimum 4 mois,** mais qu'elles **peuvent être conservées pour une durée plus longue** si cela est nécessaire (sans autre précision).

Les **données de trafic relatives aux communications entrantes dans le cadre de la fourniture de services de communications interpersonnelles**[16] doivent, pour leur part, être **conservées pendant 12 mois.**

---

[11] Dans l'Exposé des motifs, cette suppression de la liste des données de trafic qui devaient être conservées en application de l'article 122 § 2 de la loi télécom est justifiée comme suit : « *La liste des données de trafic que les opérateurs devaient traiter selon l'article 122, § 2, est supprimée, étant donné que cette liste n'est plus adaptée aux différents services de communications électroniques offerts par les opérateurs. Cette liste était surtout pertinente pour le service de téléphonie fixe […]* ».

[12] Plusieurs dispositions de la loi télécom prévoient la possibilité pour les opérateurs d'établir des profils d'utilisation des abonnés et/ou des consommateurs ou utilisateurs finaux afin de leur permettre de déterminer le plan tarifaire le plus avantageux pour eux : article 110, § 4, alinéa premier, article 110/1 et article 111, § 3, alinéa 2 de la loi télécom.

[13] L'article 122 § 3 de la loi télécom transpose l'article 6 § 3 de la Directive ePrivacy.

[14] La notion de fraude est définie par le nouvel article 122 § 4, alinéa 1er, de la loi télécom comme suit : *« un acte malhonnête fait dans l'intention de tromper en contrevenant à la loi, aux règlements ou au contrat et de se procurer ou de procurer à autrui un avantage illicite, commis par le biais de l'utilisation d'un service de communications électroniques* »

[15] La notion d'utilisation malveillante du réseau est définie par le nouvel article 122 § 4, alinéa 2, de la loi télécom comme suit : « *une utilisation du réseau afin d'importuner son correspondant ou de provoquer des dommages* ».

[16] La notion de « service de communications interpersonnelles » est issue du nouveau Code des communications électroniques européen (établi par la Directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018). Cette notion y est définie comme suit : « *un service normalement fourni contre rémunération qui permet l'échange interpersonnel et interactif direct d'informations via des réseaux de communications électroniques entre un nombre fini de personnes, par lequel les personnes qui amorcent la communication ou y participent en déterminent le ou les destinataires et qui ne comprend pas les services qui rendent possible une communication interpersonnelle et interactive uniquement en tant que fonction mineure accessoire intrinsèquement liée à un autre service* » (article 2.5) de la Directive établissant le Code des communications électroniques européen).

Aux termes du nouvel article 122 § 4 de la loi télécom**, le Roi peut – mais ne doit pas – déterminer les données de trafic qui doivent être conservées** sur pied de cette disposition.

4) Les opérateurs **doivent conserver**, pour **minimum 12 mois**[17], les **données de trafic** nécessaires **pour assurer la sécurité et le bon fonctionnement du réseau et des services de communications électroniques**, et en particulier pour détecter et analyser une atteinte potentielle ou réelle à cette sécurité, en ce compris identifier l'origine de cette atteinte (**nouvel article 122 § 4/1** de la loi télécom).

   Cette disposition donne une **définition fonctionnelle des données qui doivent être conservées** : les données de trafic nécessaires pour assurer la sécurité et le bon fonctionnement du réseau et des services de communication électroniques. Elle ne comprend **aucune définition des catégories précises de données** qui doivent être conservées et **n'habilite pas, non plus, le Roi à procéder à cette détermination**.

5) Les opérateurs **doivent conserver les données de trafic nécessaires** pour répondre à une **obligation légale** dans leur chef, pour la durée requise à cette fin (**nouvel article 122 § 4/2** de la LCE)[18].

6) Les **opérateurs de réseaux mobiles peuvent** conserver **des données de localisation autres que des données de trafic** dans les cas suivants (**nouvel article 123** de la loi télécom)[19] :

   - Lorsque cela **est nécessaire pour le bon fonctionnement et la sécurité du réseau ou du service**, les données étant conservées le temps nécessaire à cette fin ;
   - Lorsque cela est **nécessaire pour détecter ou analyser les fraudes ou l'utilisation malveillante du réseau**, les données étant conservées le temps nécessaire à cette fin ;

[17] Le nouvel article 122 § 4/1 de la loi télécom indique que les données peuvent être conservées « *pour une durée plus longue, qui est limitée au strict nécessaire* ».
[18] Dans l'Exposé des Motifs, il est indiqué à ce sujet ce qui suit : « *Un opérateur doit pouvoir conserver des données de trafic pour répondre à ses obligations légales, comme par exemple la législation comptable ou fiscale ou pour répondre à une injonction d'une autorité de geler les données (également connu comme le « quick freeze »), qui se trouve par exemple dans le Code d'instruction criminelle. Ces obligations légales ne ressortent pas du présent paragraphe mais bien des législations spécifiques qui les prévoient. Cette disposition permet également de tenir compte des évolutions futures (nouvelles obligations*) ». L'Exposé des Motifs précise ensuite que « *Conformément à l'article 15, §1er de la directive « vie privée et communications électroniques » (directive 2002/58/CE), toute obligation légale de conservation de données de trafic doit être nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour atteindre la finalité poursuivie, et adoptée dans le respect des principes généraux du droit européen, en ce compris ceux visés par la Charte des droits fondamentaux de l'Union européenne et de la Convention européenne des droits de l'homme* ».
[19] Cette disposition transpose partiellement l'article 9 de la Directive ePrivacy.

- Lorsque **les données ont été rendues anonymes** ;
- Lorsque **le traitement s'inscrit dans le cadre de la fourniture d'un service à données de trafic ou de localisation** et que l'abonné ou, le cas échéant, l'utilisateur final, **y a donné son consentement** ;
- Lorsque **le traitement est nécessaire pour répondre à une obligation légale** dans le chef de l'opérateur.

7) Les opérateurs qui offrent aux utilisateurs finaux des services de communications électroniques, ainsi que les opérateurs fournissant les réseaux de communications électroniques sous-jacents, **doivent 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**, à l'exception des données qui sont liées à une seule communication électronique (**nouvel article 126** de la loi télécom).

Ces données – à l'exception des adresses IP dynamiques, autres que celle qui a été utilisée pour souscrire au service – **sont conservées à partir de la date d'activation du service jusqu'à douze mois après la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé** (nouvel article 126 de la loi télécom).

Les **adresses IP dynamiques**, autres que celle qui a été utilisée pour souscrire au service sont, pour leur part, **conservées pendant douze mois après la fin de la session** (nouvel article 126 de la loi télécom).

Le nouvel article 126 § 2 de la loi télécom **délègue au Roi** le soin de **fixer les données à conserver** ainsi que les exigences auxquelles ces données doivent répondre. **Les articles 3 § 1, 4 § 1, 5 § 1 et 6 § 1 de l'arrêté royal du 19 septembre 2013** portant exécution des articles 126 et 126/1 de la loi du 13 juin 2005 relative aux communications électroniques et des articles 16/2/1 et 18/17/1 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (ci-après « l'arrêté du 19 septembre 2013 »), tel que modifié par le projet d'arrêté, **exécute cette habilitation législative**.

8) Les opérateurs qui offrent aux utilisateurs finaux des services de communications électroniques, ainsi que les opérateurs fournissant les réseaux de communications électroniques sous-jacents, **doivent conserver certaines données de trafic et de localisation des communications émises à partir de, ou vers, certaines zones géographiques déterminées, et ce, en principe, pour une durée de 12 mois**, à

moins qu'une autre durée soit précisée dans l'avant-projet de loi (**nouvel article 126/1** de la loi télécom).

Le nouvel article 126/1 § 1, alinéa 3, de la loi télécom précise que « *ces données sont conservées 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* ».
Le nouvel article 126/1 § 2 de la loi télécom **détermine les catégories de données qui doivent être conservées** :

- Les **données relatives à l'accès et la connexion de l'équipement terminal** au réseau **et au service et à la localisation de cet équipement**, y compris le point de terminaison du réseau ;
- Les **données de communication**, à l'exclusion du contenu, en ce compris leur origine et leur destination ;
- Les **données des appels infructueux**, pour autant que ces données soient, dans le cadre de la fourniture des services de communications concernés, générées ou traitées par les opérateurs (en ce qui concerne les données de la téléphonie) ou journalisées par les opérateurs (en ce qui concerne les données de l'internet).

Le **Roi doit fixer les données à conserver** et les exigences auxquelles ces données doivent répondre. **Les articles 3 § 2, 4 § 2, 5 § 2 et 6 § 2 de l'arrêté du 19 septembre 2013**, tel que modifié par le projet d'arrêté, **pourvoient à l'exécution** de cette habilitation.

Le nouvel article 126/1 § 3 de la loi télécom **détermine les zones géographiques** dans lesquelles les opérateurs doivent conserver les données visées au nouvel article 126/1 § 2 de la loi télécom. Il s'agit des zones géographiques suivantes :

1° **La zone géographique composée** :

- Des arrondissements judiciaires dans lesquels **au moins 3 infractions visées à l'article 90ter du CIC par 1000 habitants par an ont été constatées** durant l'année sur une moyenne des trois années calendrier précédant celle en cours
- **Des zones de police dans lesquelles, au moins 3 infractions visées à l'article 90ter du CIC par 1000 habitants par an ont été constatées** sur une moyenne des trois années calendrier précédant celle en cours, et situées dans les arrondissements judiciaires dans lesquels pendant l'année calendrier précédant celle en cours, moins de 3 infractions visées à l'article

90ter du CIC par 1000 habitants par an sur une moyenne de trois années précédant celle en cours ont été constatées.

La **durée de conservation des données varie selon le nombre d'infractions visées à l'article 90ter du CIC par an par 1000 habitants constatées** sur une moyenne des trois dernières années calendriers précédant celle en cours. Au plus ce nombre est élevé, au plus la durée de conservation est longue (la loi télécom établit trois seuils : 6 mois s'il y a 3 ou 4 infractions visées à l'article 90ter du CIC par an par 1000 habitants, 9 mois s'il y a 5 ou 6 infractions visées à l'article 90ter du CIC par an par 1000 habitants ou 12 mois s'il y a 7 ou plus de 7 infractions visées à l'article 90ter du CIC par an par 1000 habitants).

2° **Toutes les zones dont le niveau de la menace terroriste ou extrémiste**, qui est déterminé par l'Organe de coordination pour l'analyse de la menace (ci-après « l'OCAM ») **est au moins de niveau 3**. Les données doivent **être conservées aussi longtemps qu'un niveau d'au moins 3 perdure pour ces zones**.

Dans l'Exposé des motifs, il est précisé que « *Dès lors qu'un niveau de la menace atteint le niveau 3 (menace possible et vraisemblable) et, a fortiori, 4 (menace sérieuse et imminente), une conservation des données visées au § 2 [de l'article 126/1] sur les zones géographiques visées est réalisée. Il peut dans certains cas (évaluation générale de la menace de niveau 3 ou 4) s'agir de l'ensemble du territoire* »[20].

3° **Les zones particulièrement exposées à des menaces pour la sécurité nationale ou à des risques élevés de criminalité grave**. L'avant-projet de loi liste 17 catégories de lieux.

4° **Les zones où il y a une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population**. L'avant-projet liste 8 catégories de lieux (dont certaines avec des « sous-catégories » de lieux).

5° **Les zones où il y a une menace potentielle grave pour les intérêts des institutions internationales accueillies sur le territoire national**. L'avant-projet liste 6 catégories de lieux.

[20] Exposé des motifs, p. 52.

9) Les opérateurs **doivent conserver les données nécessaires pour que les autorités qui sont habilitées à obtenir l'identité des abonnés des opérateurs puissent les identifier** (**nouvel article 127** de la loi télécom).

Ces données « *sont conservées à partir de la date d'activation du service jusqu'à douze mois après la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé* » (nouvel article 127 de la loi télécom).

Cette disposition habilite (mais n'oblige pas) le Roi à déterminer les « *modalités d'identification* » de l'utilisateur final/abonné.

19. Par ailleurs, à côté des obligations de conservation préventive qui sont imposées aux opérateurs par la loi télécom, l'avant-projet de loi prévoit **d'insérer un article 39quinquies dans le CIC** afin de permettre **au procureur du Roi d'ordonner**, lors de la recherche de crimes et délits et s'il existe des indices sérieux que les infractions peuvent donner lieu à un emprisonnement correctionnel principal d'un an ou à une peine plus lourde, **la conservation, pour une durée qu'il détermine, de certaines données de trafic et de localisation** pour les besoins de l'enquête (parmi les données visées à l'article 88bis, §1, alinéa 1er du CIC[21]). La conservation doit être limitée aux seules données qui sont susceptibles de contribuer à l'élucidation de l'infraction.

❖ Quant aux possibilités pour les autorités d'accéder aux données conservées par les opérateurs

20. Le **nouvel article 127/1 de la loi télécom** comprend, comme le souligne l'Exposé des Motifs, « *la liste des catégories d'autorités qui peuvent demander l'accès aux données d'identification, aux données de trafic et aux données de localisation conservées auprès des opérateurs en vertu des [articles 122, 123, 126, 126/1 et 127] au bénéfice des autorités, des utilisateurs finaux ou pour leurs propres besoin* ».

21. Cette disposition prévoit ainsi que :

> « *Seules les autorités suivantes peuvent obtenir […] des opérateurs des données conservées en vertu des articles 122, 123, 126, 126/1 et 127, pour les finalités ci-dessous et dans les conditions prévues par les dispositions qui les y habilitent :*
> *1° les autorités compétentes pour la prévention, la recherche, la détection et la poursuite d'infractions pénales, d'infractions passibles d'une sanction administrative à caractère pénal,*

[21] Il s'agit des données suivantes : des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées et des données relatives à la localisation de l'origine ou de la destination de communications électroniques.

ou d'infractions commises à l'aide d'un réseau de communications électroniques, telles les infractions commises en ligne ;

2° 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 ;

3° les autorités chargées d'apporter de l'aide aux personnes, en ce compris le service de médiation pour les télécommunications pour ce qui concerne l'utilisation malveillante du réseau, les services d'urgence et la Cellule des personnes disparues de la Police Fédérale ;

4° l'Institut dans le cadre de la mise en œuvre et le contrôle de la présente loi ;

5° les autorités compétentes pour l'examen d'une défaillance de la sécurité du réseau ou du service ».

22. Pour déterminer à quelles données quelles autorités peuvent avoir accès et pourquoi (« **qui peut avoir accès à quoi et pourquoi ?** »), il faut, notamment, **lire le nouvel article 127/1** de la loi télécom **à la lumière des (nouvelles versions des) articles 122, 123, 126, 126/1 et 127 de la loi télécom** :

- Les **autorités qui poursuivent l'une des finalités** visées à l'article 127/1 de la loi télécom[22] **peuvent avoir accès aux données conservées en vertu des** (nouvelles versions des) **articles 122, 123, 126 et 127 pour chacune des finalités énoncées par cet article 127/1** de la loi télécom. Les autorités compétentes pour poursuivre l'une des finalités énoncées par le nouvel article 127/1 de la loi télécom **peuvent donc avoir accès à toutes les données qui sont conservées en application des articles 122 et 123, 126 et 127 de la loi télécom**, même si leur conservation a initialement été autorisée ou imposée pour une autre finalité que celle qui est poursuivie par l'autorité qui veut obtenir l'accès auxdites données[23].

- Les **autorités qui poursuivent l'une des finalités** visées à l'article 127/1 de la loi télécom **peuvent avoir accès aux données conservées en vertu du nouvel**

[22] Contrairement aux versions antérieures de la loi télécom, le nouvel article 127/1 reprend une liste des finalités pour lesquelles les autorités peuvent obtenir un accès aux données conservées, et non plus une liste d'autorités pouvant avoir accès aux données. L'Exposé des Motifs justifie ce changement de perspective comme suit : « *Cela permet d'assurer que la législation couvre les différents cas de figure et les évolutions futures. A cet égard, il convient de noter qu'il est rapidement apparu que la liste fermée des autorités visées à l'article 126, § 2 était incomplète. L'adaptation de cette liste fermée s'est révélée être un exercice difficile (par exemple car la loi est attaquée devant la Cour constitutionnelle et peut difficilement être modifiée) et très lent, alors que le fait pour une autorité de ne pas figurer sur la liste, alors que c'est nécessaire, provoque immédiatement des difficultés opérationnelles pour cette dernière. Les données d'identification et de souscription visées par les articles 126 et 127 sont des données basiques dont ont besoin un nombre non négligeable d'autorités. On peut s'attendre à ce que ce nombre augmente à l'avenir, étant donné la croissance du nombre d'infractions en ligne. Il est également très difficile de faire une liste exhaustive de toutes les dispositions légales qui permettent aux différentes autorités d'obtenir des opérateurs des données d'identification, de trafic ou de localisation* ».

[23] En effet, les nouveaux articles 122 § 7 et 123 § 6 de la loi télécom prévoient, chacun, que « *cet article [à savoir, respectivement, l'article 122 et l'article 123] ne porte pas préjudice à l'article 127/1* ». Le nouvel article 126 § 1, alinéa 3, prévoit que « Ces données sont conservées pour les autorités et les finalités visées à l'article 127/1 » et le nouvel article 127 § 1, alinéa 2, prévoit que « *Ces données et documents sont conservés pour les autorités et les finalités visées à l'article 127/1* ».

article 126/1 de la loi télécom **uniquement pour les finalités pour lesquelles elles sont conservées**, à savoir aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique et de la sauvegarde des intérêts vitaux d'une personne physique.

23. Il faut préciser, en outre, que pour qu'une autorité puisse obtenir des données de l'opérateur, il est nécessaire **qu'elle poursuive l'une des finalités visées à l'article 127/1** de la loi télécom **et** que **sa loi organique ou sectorielle lui donne le pouvoir d'obtenir ces données de l'opérateur**[24].

24. L'avant-projet de loi entend d'ailleurs **modifier plusieurs dispositions déterminant dans quelles conditions certaines autorités peuvent avoir accès aux données** de trafic et/ou de localisation conservées par les opérateurs :

- L'avant-projet prévoit d'intégrer un **§ 2, 2°/1 à l'article 14 de la loi statut IBPT** afin de permettre à l'IBPT de « *demander aux opérateurs les données d'identification, de trafic ou de localisation, au sens de la loi du 13 juin 2005 relative aux communications électroniques, pour autant que cela soit nécessaire à l'accomplissement de l'une de ses missions* ».

- **L'article 88bis du CIC** permet au juge d'instruction, « *s'il existe des indices sérieux que les infractions sont de nature à entraîner un emprisonnement correctionnel principal d'un an ou une peine plus lourde, et lorsque le juge d'instruction estime qu'il existe des circonstances qui rendent le repérage de communications électroniques ou la localisation de l'origine ou de la destination de communications électroniques nécessaire à la manifestation de la vérité, il peut faire procéder au repérage des données de trafic de moyens de communication électronique à partir desquels ou vers lesquels des communications électroniques sont adressées ou ont été adressées [et] à la localisation de l'origine ou de la destination de communications électroniques* ». L'avant-projet **y réintroduit un paragraphe 3**, qui a été annulé par la Cour constitutionnelle dans son arrêt n° 57/2021. Ce paragraphe établit **des règles particulières concernant le repérage des données relatives aux moyens de communications électroniques des avocats et des médecins**, étant donné que ces personnes sont tenues au secret professionnel.

- Le nouvel **article 42 § 2 de la loi sur la fonction de police** prévoit que *« Un officier de police judiciaire de la Cellule des Personnes Disparues de la police fédérale*

[24] L'article 127/1 prévoit, en effet, que « Seules les autorités suivantes peuvent obtenir […] des opérateurs des données conservées en vertu des articles 122, 123, 126, 126/1 et 127, pour les finalités ci-dessous et dans les conditions prévues par les dispositions qui les y habilitent » (c'est l'Autorité qui souligne).

peut, dans le cadre de sa mission d'assistance à personne en danger et de recherche de personnes dont la disparition est inquiétante, et lorsqu'il existe des présomptions ou indices sérieux que l'intégrité physique de la personne disparue se trouve en danger imminent, requérir d'obtenir les données relatives aux communications électroniques concernant la personne disparue […] ».

- La **loi sur les services de renseignement** qui détermine les conditions auxquelles ces services peuvent avoir accès aux données conservées par les opérateurs

- **L'article 84 § 1 de la loi FSMA** prévoit que « *moyennant l'autorisation préalable d'un juge d'instruction, l'auditeur ou, en son absence l'auditeur adjoint, peut, lorsqu'il estime qu'il existe des circonstances qui rendent le repérage de communications électroniques ou la localisation de l'origine ou de la destination de communications électroniques nécessaire à la manifestation de la vérité, faire procéder : 1° au repérage des données de trafic de moyens de communications électroniques à partir desquels ou vers lesquels des communications électroniques ont été faites ; 2° à la localisation de l'origine ou de la destination de communications électroniques, y compris les numéros de téléphone et les adresses réseau ; 3° à la demande des détails de paiement des services de communications électroniques […]. L'auditeur ou, en son absence l'auditeur adjoint, indique dans sa décision les circonstances de fait qui justifient la mesure prise et il tient compte, pour motiver sa décision, des principes de proportionnalité et de subsidiarité. […]* ». L'avant-projet prévoit **d'ajouter un nouveau § 1er bis/1** à l'article 84 de la loi FSMA **qui permet à l'auditeur d'ordonner aux opérateurs de conserver certaines données au cas où ces données risquent d'être supprimées ou rendues anonymes,** jusqu'à ce qu'il ait obtenu d'un juge d'instruction l'autorisation de requérir la communication de ces données.

- L'avant-projet entend permettre aux « *membres du personnel statutaire ou contractuel du Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement désignés à cette fin par le Roi* », qui sont chargés de surveiller l'exécution de la loi relative à la protection de la santé et de ses arrêtés d'exécution ainsi que des règlements de l'Union européenne et qui relèvent des compétences du Service public fédéral Santé publique, Sécurité de la Chaîne alimentaire et Environnement, « *identifier les personnes physiques et morales sur la base de leur numéro de téléphone ou de l'adresse IP à la source de la communication électronique* ». **Le nouvel article 11 § 1 de la loi relative à la protection de la santé** prévoira désormais que ces membres du personnel statutaire ou contractuel

du Service public fédéral Santé publique, Sécurité de la chaîne alimentaire et Environnement pourront « *sur requête dûment motivée, demander la mise à disposition de documents et de données d'identification […]* ».

- L'avant-projet entend ajouter **un § 2 à l'article 62 de la loi NIS** afin de permettre au Centre pour la Cybersécurité Belgique (ci-après « le CCB ») « [l*]orsque cela s'avère strictement nécessaire à la réalisation de ses tâches énumérées à l'article 60, a) à e), de la présente loi, [d'] obtenir des opérateurs […] des données d'identification, de trafic ou de localisation conservées par ceux-ci […]* »[25].

C. RAPPEL DES CONDITIONS AUXQUELLES DOIVENT REPONDRE LES NORMES QUI PREVOIENT UNE CONSERVATION DES DONNEES DE TRAFIC ET/OU LOCALISATION ET LEUR COMMUNICATION EVENTUELLE AUX AUTORITES

25. La **conservation des données** relatives au trafic et des données de localisation **constitue une ingérence importante dans les droits au respect de la vie privée et à la protection des données à caractère personnel.** En effet, comme la CJUE l'a souligné, à plusieurs reprises, « *les données relatives au trafic et les données de localisation sont susceptibles de révéler des informations sur un nombre important d'aspects de la vie privée des personnes concernées, y compris des informations sensibles, telles que l'orientation sexuelle, les opinions politiques, les convictions religieuses, philosophiques, sociétales ou autres ainsi que l'état de santé, alors que de telles données jouissent, par ailleurs, d'une protection particulière en droit de l'Union. Prises dans leur ensemble, lesdites données peuvent permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci. En particulier, ces données fournissent les moyens d'établir le profil des personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications* »[26].

26. **La communication** éventuelle de ces données aux autorités **constitue une ingérence distincte** de celle qui est causée par leur conservation**,** mais qui est, elle aussi, **importante**.

---

[25] Les tâches énumérées à l'article 60 a) à e) de la loi NIS sont les suivantes :
« *a) le suivi des incidents au niveau national et international, en ce compris le traitement de données à caractère personnel lié au suivi de ces incidents ;*
b) l'activation du mécanisme d'alerte précoce, la diffusion de messages d'alerte, les annonces et la diffusion d'informations sur les risques et incidents auprès des parties intéressées ;
c) l'intervention en cas d'incident ;
d) l'analyse dynamique des risques et incidents et conscience situationnelle ;
e) la détection, l'observation et l'analyse des problèmes de sécurité informatique »

[26] Voyez, par exemple, CJUE, 8 avril 2014, *affaires jointes C-293/12 et C-594/12 « Digital Rights Irland* et *al* », § 27 ; CJUE, 21 décembre 2016, *affaires jointes C-203/15 et C-698/15 « Tele2 Sverige et al »*, § 99 ; CJUE, 2 octobre 2020, *affaires jointes C-511/18, C-512/18 et C-520/18 « Quadrature du Net et al »*, § 117.

27. L'Autorité rappelle que toute ingérence dans le droit au respect de la protection des données à caractère personnel, en particulier lorsque l'ingérence s'avère importante comme c'est le cas en l'espèce, n'est admissible que **si elle encadrée par une norme suffisamment claire et précise et dont l'application est prévisible pour les personnes concernées.** Ainsi, toute norme encadrant des traitements de données à caractère personnel, en particulier lorsque ceux-ci constituent une ingérence importante dans les droits et libertés des personnes concernées, doit répondre **aux exigences de prévisibilité et de précision** de sorte qu'à sa lecture, **les personnes concernées, puissent entrevoir clairement les traitements qui sont faits de leurs données et les circonstances dans lesquelles un traitement de données est autorisé**. En exécution de l'article 6.3 du RGPD, lu en combinaison avec les articles 22 de la Constitution et 8 de la Convention européenne des droits de l'homme et des libertés fondamentales, les **éléments essentiels du traitement** doivent y être **décrits avec précision**. Il s'agit, en particulier, de la ou des **finalité(s)** précise(s) du traitement ; de **l'identité du (ou des) responsable(s) du traitement** ; des **catégories de données traitées**, étant entendu que celles-ci doivent s'avérer – conformément à l'article 5.1. du RGPD, « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées* » ; des **catégories de personnes concernées** (personnes à propos desquelles des données seront traitées) ; de la **durée de conservation des données** ; des destinataires ou **catégories de destinataires** auxquels leurs données sont communiquées et les **circonstances dans lesquelles et les raisons pour lesquelles elles seront communiquées** ainsi que **toutes mesures visant à assurer un traitement licite et loyal de ces données à caractère personnel**.

28. Outre l'exigence de légalité, une ingérence dans le droit au respect de la protection des données n'est admissible que si elle est **nécessaire** et **proportionnée** à l'(aux) objectif(s) qu'elle poursuit. À travers plusieurs arrêts se prononçant sur la conformité de la conservation des données de trafic et de localisation et leur communication ultérieure éventuelle aux autorités avec les droits au respect de la vie privée et à la protection des données à caractère personnel[27], la **CJUE a clarifié la portée de ces exigences de nécessité et de proportionnalité**. Ce faisant, la Cour de Luxembourg **a clarifié les conditions** que doivent rencontrer les mesures législatives qui imposent **une conservation des données de trafic et de localisation** et **leur communication éventuelle aux autorités**, en particulier à des fins répressives.

29. Les règlementations qui prévoient une conservation des données doivent opérer une **pondération équilibrée** entre, d'une part, **l'objectif d'intérêt général** poursuivi par l'ingérence et, d'autre part, **les droits au respect de la vie privée et à la protection des données à caractère personnel**.

[27] Voyez, en particulier, CJUE, 8 avril 2014, *affaires jointes C-293/12 et C-594/12 « Digital Rights Irland et al »*; CJUE, 21 décembre 2016, *affaires jointes C-203/15 et C-698/15 « Tele2 Sverige et al »* ; CJUE, 2 octobre 2018, *affaire C-207/16 Ministerio Fiscal* ; CJUE, 2 octobre 2020, *affaires jointes C-511/18, C-512/18 et C-520/18 « Quadrature du Net et al »* ; CJUE, 2 mars 2021, *affaire C-746/18* « *Prokuratuur »*.

Il convient ainsi de **vérifier que la gravité de l'ingérence est en relation avec l'importance de l'objectif d'intérêt général poursuivi**[28]. En d'autres termes, **au plus l'objectif d'intérêt général poursuivi est important, au plus la règlementation imposant une conservation des données peut être intrusive** dans les droits et libertés des personnes concernées. Mais quoi qu'il en soit, **la conservation des données de trafic et de localisation doit**, dans une société démocratique, **rester l'exception**[29]. Ces données ne peuvent donc pas faire l'objet d'une conservation systématique et continue, quand bien même une telle conservation permettrait de lutter contre la criminalité grave et prévenir des menaces graves contre la sécurité publique. La Cour de justice estime, en effet, qu'une **mesure de conservation généralisée et indifférenciée des données** constitue une **ingérence tellement importante** dans les droits fondamentaux des personnes concernées qu'elle **n'est, en principe, pas admissible**[30] (sauf, nous y reviendrons, à des fins de sauvegarde de la sécurité nationale[31]).

30. De plus, la CJUE exige que les règlementations qui prévoient une conservation des données **répondent à des critères objectifs** et **établissent un rapport entre les données à conserver et l'objectif poursuivi**[32].

31. Appliquant le principe de proportionnalité lors de l'examen de différentes catégories de mesures imposant une conservation des données de trafic et/ou de localisation, **la Cour a identifié les conditions dans lesquelles de telles mesures étaient – ou non – admissibles**.

- ***Mesures imposant une conservation généralisée et indifférenciée des données à des fins de sauvegarde de la sécurité nationale***

32. L'objectif de **sauvegarde de la sécurité nationale** est d'une telle importance que la CJUE admet **qu'il puisse justifier une conservation généralisée et indifférenciée** des données de localisation et de trafic, **à condition** qu'il existe une **menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible** (et **uniquement** pour la p**ériode pendant laquelle cette menace existe**)[33].

33. La Cour ajoute qu'il est essentiel que la **décision qui enjoint** aux fournisseurs de services de communications électroniques **de procéder à une telle conservation** des données puisse faire l'objet d'un **contrôle effectif** soit par une juridiction, soit par une entité administrative indépendante,

[28] CJUE, arrêt du 2 octobre 2018, § 55 ; CJUE, arrêt du 6 octobre 2020, § 131 ; CJUE, arrêt du 2 mars 2021, § 32.
[29] CJUE, arrêt du 6 octobre 2020, § 142.
[30] CJUE, arrêt du 6 octobre 2020, § 141.
[31] CJUE, arrêt du 6 octobre 2020, § 136-137.
[32] CJUE, arrêt du 6 octobre 2020, § 133.
[33] CJUE, arrêt du 6 octobre 2020, § 137.

dont la décision est dotée d'un effet contraignant, visant à **vérifier l'existence d'une de ces situations** ainsi que **le respect des conditions et des garanties devant être prévues**[34].

- ***Mesures imposant une conservation préventive ciblée des données de trafic et des données de localisation à des fins de lutte contre la criminalité grave et prévention contre des menaces graves à la sécurité publique***

34. Selon la CJUE, une **conservation généralisée et indifférenciée** des données relatives au trafic et à la localisation **en vue de lutter contre la criminalité, même grave, excède,** dans une société démocratique, **ce qui est nécessaire**[35]. Les Etats **ne** peuvent donc **pas imposer une conservation généralisée et indifférenciée de ces données pour lutter contre la criminalité grave**. *A fortiori,* une telle mesure ne peut être introduite pour prévenir, rechercher, détecter et poursuivre des infractions pénales en général[36]. En revanche, la Cour estime qu'une **conservation préventive ciblée** des données de trafic et de localisation afin **de lutter contre la criminalité grave**, prévenir **des atteintes graves à la sécurité publique** et, *a fortiori*, **sauvegarder la sécurité nationale** peut être justifiée[37]. La lutte contre la criminalité en général ne peut, en revanche, pas justifier une telle conservation préventive, même si elle est ciblée.

35. Selon la Cour, **plusieurs critères** peuvent être utilisés **pour cibler la conservation** préventive des données en vue de **lutter contre la criminalité grave** : la conservation peut être limitée à des **données afférentes à une période temporelle** et/ou **une zone géographique** et/ou **sur un cercle de personnes** susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer par la conservation de leurs données, à la lutte contre la criminalité grave[38].

36. Quant à la délimitation de la conservation des données sur base de **critères géographiques**, la CJUE considère qu'elle est admise lorsque les autorités nationales compétentes considèrent, **sur la base d'éléments objectifs et non discriminatoires**, qu'il existe, dans une ou plusieurs zones géographiques, une **situation caractérisée par un risque élevé de préparation ou de commission d'actes de criminalité grave**. La Cour précise que « *[c]es zones peuvent être, notamment, des lieux caractérisés par un nombre élevé d'actes de criminalité grave, des lieux particulièrement exposés à la commission d'actes de criminalité grave, tels que des lieux ou infrastructures fréquentés régulièrement par un nombre très élevé de personnes, ou encore des lieux stratégiques, tels que des aéroports, des gares ou des zones de péages* »[39].

[34] CJUE, arrêt du 6 octobre 2020, § 139.
[35] CJUE, arrêt du 6 octobre 2020, § 141.
[36] CJUE, arrêt du 6 octobre 2020, § 140.
[37] CJUE, arrêt du 6 octobre 2020, § 146-151.
[38] CJUE, arrêt du 8 avril 2014, § 59 ; CJUE, arrêt 21 décembre 2016, § 106 ; CJUE, arrêt du 6 octobre 2020, § 144.
[39] CJUE, arrêt du 6 octobre 2020, § 150.

37. Dans tous les cas, **les mesures imposant une conservation ciblée** des données à des fins de lutte contre la criminalité grave **ne sauraient dépasser celle qui est strictement nécessaire** au regard de l'objectif poursuivi ainsi que **des circonstances** la justifiant, sans préjudice d'un renouvellement éventuel en raison de la persistance de la nécessité de procéder à une telle conservation.

- ***Mesures imposant une conservation préventive et généralisée des adresses IP à des fins de lutte contre la criminalité grave et la sauvegarde de la sécurité publique***

38. La CJUE relève que « *les adresses IP, quoique faisant partie des données relatives au trafic, sont générées sans être rattachées à une communication déterminée et servent principalement à identifier, par l'intermédiaire des fournisseurs de services de communications électroniques, la personne physique propriétaire d'un équipement terminal à partir duquel une communication au moyen de l'Internet est effectuée* »[40]. Pour autant que seules les adresses IP de la source des communications soient conservées et non celles du destinataire de celles-ci, ces adresses IP ne révèlent pas, en tant que telles, des informations sur le(s) destinataire de la communication[41]. Les adresses IP attribuées à la source d'une connexion présentent ainsi, selon la CJUE, un degré de sensibilité moindre que les autres données relatives au trafic, mais la CJUE souligne que ces adresses IP peuvent néanmoins être utilisées – si elles sont combinées aux adresses IP du destinataire de la communication – pour effectuer le traçage exhaustif du parcours de navigation d'un internaute et, par suite, de son activité en ligne, ces données permettent d'établir le profil détaillé de ce dernier[42]. **La conservation et l'analyse de ces données constituent dès lors des ingérences graves dans les droits fondamentaux de l'internaute[43]**.

39. Elle estime toutefois qu'il **est admissible d'imposer une conservation de ces données généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion**[44], **pourvu que cette possibilité soit soumise au strict respect des conditions matérielles et procédurales devant régir l'utilisation de ces données[45]**. Eu égard à la gravité de l'ingérence causée par la conservation généralisée et indifférenciée des adresses IP, la CJUE estime que **seule la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique sont de nature,** à l'instar de la sauvegarde de la sécurité nationale, **à justifier cette ingérence[46]**. La Cour ajoute que la **durée de conservation** doit être **limitée à ce qui est**

[40] CJUE, arrêt du 6 octobre 2020, § 152.
[41] CJUE, arrêt du 6 octobre 2020, § 152.
[42] CJUE, arrêt du 6 octobre 2020, § 152-153.
[43] CJUE, arrêt du 6 octobre 2020, § 153.
[44] En effet, la Cour note que, dans le cas d'une infraction commise en ligne, l'adresse IP peut constituer le seul moyen d'investigation permettant l'identification de la personne à laquelle cette adresse était attribuée au moment de la commission de cette infraction. Or, la conservation des adresses IP par les fournisseurs de services de communications électroniques au-delà de la durée d'attribution de ces données n'apparaît, en principe, pas nécessaire aux fins de la facturation des services en cause, de telle sorte que la détection des infractions commises en ligne peut, de ce fait, s'avérer impossible sans avoir recours à une mesure législative imposant la conservation de ces données.
[45] CJUE, arrêt du 6 octobre 2020, § 155.
[46] CJUE, arrêt du 6 octobre 2020, § 156.

strictement nécessaire au regard de l'objectif poursuivi[47]. Enfin, il est nécessaire de prévoir **des conditions et des garanties strictes** quant à l'exploitation de ces données, notamment par un traçage, à l'égard des communications et des activités effectuées en ligne par les personnes concernées[48].

- ***Mesures imposant une conservation généralisée et indifférenciée des données relatives à l'identité civile***

40. La CJUE souligne que les **données relatives à l'identité civile** des utilisateurs des moyens de communications ne permettent pas, à elles seules, de connaître la date, l'heure, la durée et les destinataires des communications effectuées, les endroits où ces communications ont eu lieu ou la fréquence de celles-ci avec certaines personnes pendant une période donnée[49]. Il s'ensuit que **l'ingérence causée par la conservation de ces données ne doit pas être qualifiée de grave[50]**. La Cour estime dès lors qu'une mesure législative peut imposer, sans délai particulier, **la conservation des données relatives à l'identité civile de l'ensemble des utilisateurs** des moyens de communications électroniques **aux fins de la prévention, de la recherche, de la détection et de la poursuite d'infractions pénales** ainsi que de la **sauvegarde de la sécurité publique**, sans qu'il soit nécessaire que les infraction pénales ou que les menaces contre ou les atteintes à la sécurité publique soient graves[51].

- ***Mesures imposant une conservation « rapide » des données de trafic et de localisation à des fins de lutte contre la criminalité grave***

41. Les données de trafic et de localisation, qui sont conservées et traitées par les fournisseurs de services de communications électroniques sur la base des articles 5, 6, 9 ou 15 de la Directive ePrivacy, doivent, en principe, être effacées ou rendues anonymes au terme de délais légaux déterminés par les dispositions nationales transposant la Directive ePrivacy[52]. La CJUE reconnait toutefois **qu'il peut être nécessaire de conserver ces données au-delà de ces délais** « *aux fins de l'élucidation d'infractions pénales graves ou d'atteintes à la sécurité nationale, et ce tant dans la situation où ces infractions ou ces atteintes ont déjà pu être constatées que dans celle où leur existence peut, au terme d'un examen objectif de l'ensemble des circonstances pertinentes, être raisonnablement soupçonnée* »[53].

[47] CJUE, arrêt du 6 octobre 2020, § 156
[48] CJUE, arrêt du 6 octobre 2020, § 156.
[49] CJUE, arrêt du 6 octobre 2020, § 157 ; CJUE, arrêt du 2 mars 2021, § 34.
[50] CJUE, arrêt du 6 octobre 2020, § 157.
[51] CJUE, arrêt du 6 octobre 2020, § 158.
[52] CJUE, arrêt du 6 octobre 2020, § 160.
[53] CJUE, arrêt du 6 octobre 2020, § 161.

42. La Cour de Luxembourg admet ainsi que les Etats **peuvent prévoir**, dans leur législation, **la possibilité d'enjoindre** aux fournisseurs de services de communications électroniques **de procéder**, pour une durée déterminée, à **la « conservation rapide »** des données relatives au trafic et des données de localisation dont ils disposent en vertu de dispositions législatives transposant les articles 5, 6, 9 et 15 de la Directive ePrivacy[54]. Une mesure de « conservation rapide » peut ainsi être prise à l'égard de données dont la conservation initiale poursuivait une autre finalité que la lutte contre la criminalité grave ou la sauvegarde de la sécurité nationale.

43. Toutefois, **la décision** de faire procéder à une conservation rapide des données n'est admise qu'aux **conditions suivantes**[55] :

- Cette décision doit être **soumise à un contrôle juridictionnel effectif ;**

- Cette décision ne peut être prise **qu'en vue de lutter contre la criminalité grave** et, *a fortiori*, la **sauvegarde de la sécurité nationale ;**

- L'obligation de conservation **ne peut porter que sur les données** de trafic et données de localisation **susceptibles de contribuer à l'élucidation de l'infraction pénale grave ou de l'atteinte à la sécurité nationale concernée[56]** ;

- La **durée de conservation** de ces données doit être **limitée au strict nécessaire**, celle-ci pouvant néanmoins être prolongée lorsque les circonstances et l'objectif poursuivi par ladite mesure le justifient.

➢ ***Exigences relatives aux mesures techniques et organisationnelles concernant la conservation des données par les fournisseurs de services de communications électroniques.***

44. La CJUE souligne qu'aux termes de l'article 4 §§ 1 et 1bis de la Directive ePrivacy, les fournisseurs doivent prendre des **mesures d'ordre technique et organisationnel appropriées** pour assurer **une protection efficace des données** conservées **contre les risques d'abus** ainsi que **contre**

[54] CJUE, arrêt du 6 octobre 2020, § 163.
[55] CJUE, arrêt du 6 octobre 2020, § 164.
[56] À cet égard, la CJUE admet que la conservation rapide des données peut concerner les données des personnes concrètement soupçonnées d'avoir commis une infraction pénale ou une atteinte à la sécurité nationale, mais également les *« données […] afférentes à des personnes autres que celles qui sont soupçonnées d'avoir projeté ou commis une infraction pénale grave ou une atteinte à la sécurité nationale, pour autant que ces données peuvent, sur la base d'éléments objectifs et non discriminatoires, contribuer à l'élucidation d'une telle infraction ou d'une telle atteinte à la sécurité nationale, telles que les données de la victime de celle-ci, de son entourage social ou professionnel, ou encore de zones géographiques déterminées, telles que les lieux de la commission et de la préparation de l'infraction ou de l'atteinte à la sécurité nationale en cause* » (CJUE, arrêt du 6 octobre 2020, § 165).

tout accès illicite à ces données[57]. La Cour insiste, en particulier, sur la nécessité pour la réglementation nationale de **prévoir la conservation sur le territoire de l'Union** ainsi que la **destruction irrémédiable des données** au terme de la durée de conservation de celles-ci[58]. Il faut, en outre, que les **Etats garantissent le contrôle, par une autorité indépendante, du respect du niveau de protection garanti** par le droit de l'Union en matière de protection des personnes physiques à l'égard du traitement des données à caractère personnel.

- ***Sur l'accès aux données conservées par les fournisseurs de services de communications électroniques***

45. Conformément à l'exigence de prévisibilité, la communication des données conservées par les fournisseurs de services de communications électroniques aux autorités nationales **doit être encadrée par des règles claires et précises** indiquant les **circonstances** et **sous quelles conditions** cette communication a lieu. Cette règlementation doit prévoir **des conditions matérielles et procédurales** afin de garantir que l'accès aux données conservées soit limité au strict nécessaire[59] **:**

    - **La règlementation doit déterminer la finalité pour laquelle les autorités peuvent obtenir un accès aux données conservées par les fournisseurs de services de communication**. À cet égard, la Cour indique que **l'accès aux données ne peut, en principe, être justifiée que par l'objectif d'intérêt général pour lequel leur conservation a été imposée**[60]. Ainsi, un accès à des fins de poursuite et de sanction d'une infraction pénale ordinaire ne saurait en aucun cas être accordé lorsque leur conservation a été justifiée par l'objectif de lutte contre la criminalité grave ou, *a fortiori*, de sauvegarde de la sécurité nationale. **En revanche**, conformément au principe de **proportionnalité**, un **accès à des données conservées en vue de la lutte contre la criminalité grave peut**, pour autant que soient respectées les conditions matérielles et procédurales entourant un tel accès, **être justifié par l'objectif de sauvegarde de la sécurité nationale**. En outre, la Cour admet que les **Etats peuvent prévoir que des données conservées d'une manière conforme aux articles 5, 6, 9 ou 15 de la Directive ePrivacy** peuvent être communiquées aux autorités, dans le respect de conditions matérielles et procédurales, **à des fins de lutte contre la criminalité grave ou de sauvegarde de la sécurité nationale**[61].

[57] CJUE, arrêt du 21 décembre 2016, § 122.
[58] CJUE, arrêt du 21 décembre 2016, § 122.
[59] CJUE, arrêt du 21 décembre 2016, §§ 118-121.
[60] CJUE, arrêt du 2 mars 2021, § 31.
[61] CJUE, arrêt du 6 octobre 2020, § 164-165.

La règlementation régissant l'accès aux données doit donc déterminer la finalité poursuivie par les autorités pouvant avoir accès aux données, mais cette règlementation ne saurait se limiter à exiger que l'accès réponde à l'un des objectifs visés par l'article 15 § 1 de la Directive ePrivacy, fût-ce la lutte contre la criminalité grave[62]. Cette règlementation doit également prévoir des conditions matérielles et procédurales régissant cette utilisation[63].

- **La réglementation nationale concernée doit se fonder sur des critères objectifs pour définir les circonstances et les conditions dans lesquelles l'accès aux données doit être accordé[64]**. À cet égard, un accès ne saurait, en principe, être accordé, en relation avec l'objectif de lutte contre la criminalité, qu'aux données de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction grave ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction. Toutefois, dans des situations particulières, telles que celles dans lesquelles des intérêts vitaux de la sécurité nationale, de la défense ou de la sécurité publique sont menacés par des activités de terrorisme, l'accès aux données d'autres personnes pourrait également être accordé lorsqu'il existe des éléments objectifs permettant de considérer que ces données pourraient, dans un cas concret, apporter une contribution effective à la lutte contre de telles activités.

- **L'accès des autorités nationales** compétentes aux données conservées doit, en principe, sauf cas d'urgence dûment justifiés, **être subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante**. La décision de cette juridiction ou de cette entité **doit intervenir à la suite d'une demande motivée de ces autorités**[65]. Par ailleurs, la Cour a souligné que **l'autorité chargée d'exercer le contrôle préalable**, qu'il s'agisse d'une juridiction ou d'une entité administrative indépendante, doit avoir **la qualité de tiers** par rapport à celle qui demande l'accès aux données, afin que la première puisse exercer ce contrôle de manière impartiale, à l'abri de toute influence extérieure[66].

- Les autorités qui ont eu accès aux données **doivent en informer les personnes concernées dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes** menées par ces autorités. En effet, cette information est, de fait, nécessaire pour permettre aux personnes concernées d'exercer,

[62] CJUE, arrêt du 21 décembre 2018, § 118.
[63] CJUE, arrêt du 2 mars 2021, § 49.
[64] CJUE, arrêt du 2 mars 2021, § 50.
[65] CJUE, arrêt du 21 décembre 2018, § 120 ; CJUE, arrêt du 2 mars 2021, § 51.
[66] CJUE, arrêt du 2 mars 2021, § 52.

notamment, le droit de recours, explicitement prévu à l'article 15 § de la directive ePrivacy, lu en combinaison avec le RGPD, en cas de violation de leurs droits[67].

D. EXAMEN DE LA CONFORMITE DE L'AVANT-PROJET DE LOI ET DU PROJET D'ARRETE AVEC LES EXIGENCES DU DROIT EUROPEEN ET DES PRINCIPES FONDAMENTAUX EN MATIERE DE PROTECTION DES DONNEES

46. L'Autorité examine ci-dessous les différentes dispositions de l'avant-projet de loi qui autorisent ou imposent la conservation de données de trafic et/ou de localisation en vue de leur communication éventuelle aux autorités, afin d'apprécier leur conformité avec les principes fondamentaux en matière de protection des données.

47. L'Autorité estime nécessaire, préalablement à cet examen, de rappeler, comme la Cour constitutionnelle l'a fait dans son arrêt du 21 avril 2021, que la jurisprudence de la CJUE « *impose un changement de perspective par rapport au choix que le législateur a effectué* » : **l'obligation de conservation des données de trafic et de localisation doit être l'exception, et non la règle**. Or force est de constater que **l'avant-projet de loi** – qui entend répondre à l'annulation de la loi de 2016 **– n'opère pas complètement ce changement de perspective** puisque, comme l'Autorité le développera ci-dessous, l'avant-projet de loi entend imposer de nouvelles mesures de conservation des données de trafic et de localisation (afin de lutter 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. **L'Autorité insiste pour que le législateur adapte l'avant-projet de loi pour que la loi qui sera votée respecte toutes les exigences imposées par la CJUE et la Cour constitutionnelle**. Il s'agit d'une condition essentielle pour conserver la confiance des citoyennes et des citoyens.

48. L'Autorité est consciente que la conservation des données de trafic et de localisation peut être nécessaire pour garantir le droit à la sécurité et le droit à un recours effectif qui sont, comme le droit au respect de la vie privée et à la protection des données à caractère personnel, des droits fondamentaux consacrés par la Constitution belge, la Convention européenne des droits de l'homme et la Charte des droits fondamentaux de l'Union européenne. La CJUE, dans son arrêt du 6 octobre 2020, reconnait d'ailleurs la nécessité de procéder à une conciliation entre ces différents droits fondamentaux[68]. Elle rappelle, dans ce contexte, qu' « *un objectif d'intérêt général ne saurait être poursuivi sans tenir compte du fait qu'il doit être concilié avec les droits fondamentaux concernés par la mesure, ce en effectuant une pondération équilibrée entre d'une part, l'objectif d'intérêt général et, d'autre, part, les droits en cause* »[69]. Dans l'analyse de la proportionnalité des différentes mesures de

[67] CJUE, arrêt du 21 décembre 2018, § 121.
[68] CJUE, arrêt du 6 octobre 2020, § 127.
[69] CJUE, arrêt du 6 octobre 2020, § 130.

conservation des données de trafic et de localisation, la CJUE a ainsi cherché constamment à réaliser cette conciliation entre les différents droits fondamentaux en jeu. **L'Autorité invite le législateur à prendre le temps de la réflexion et de l'analyse rigoureuse pour concilier, dans le respect de la jurisprudence européenne, les droits fondamentaux à la sécurité et à un recours effectif, d'une part, et les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, d'autre part**.

1) Remarque préalable concernant l'interaction entre l'avant-projet de loi et le Code de communications électroniques européen

49. Certaines modifications apportées par l'avant-projet de loi aux articles 122 et suivants de la loi télécom et par le projet d'arrêté visent à aligner la terminologie qu'ils emploient avec celle du Code de communications électroniques européen (ci-après « CCEE »). Ainsi, l'avant-projet de loi ou le projet d'arrêté utilisent, sans les définir, plusieurs notions qui ne sont pas encore définies (en particulier les notions de « service de communications interpersonnelles » ou de « services nomades ») parce qu'il est prévu que la loi télécom définisse ces notions à la suite de sa modification par la loi qui transposera le CCCE en droit interne. Le délégué du Ministre a confirmé que ce texte était en cours de finalisation et qu'il devrait être déposé au Parlement avant les vacances parlementaires. L'Autorité en prend note et souligne que **si le texte, qui définit ces nouvelles notions, n'était pas adopté avant l'adoption de l'avant-projet de loi et du projet d'arrêté, il conviendra d'inclure les définitions des notions qu'ils utilisent dans l'avant-projet de lo**i.

50. Par ailleurs, l'Autorité souligne **que la transposition du CCEE va entrainer la redéfinition, notamment, des concepts d'« opérateurs » et de « services de communications électroniques »**. La notion de « service de communications électroniques » sera désormais 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 consistant entièrement ou principalement en la transmission de signaux, tels que les services de transmission utilisés pour la fourniture de services de machine à machine* ». La notion de « service de communications électroniques » sera donc définie de manière beaucoup plus large qu'actuellement puisqu'elle va englober, en particulier, les « services de communications interpersonnelles » qui seront définis comme : « *un service normalement fourni contre rémunération qui permet l'échange interpersonnel et interactif direct d'informations via des réseaux de communications électroniques entre un nombre fini de personnes, par lequel les personnes qui amorcent la communication ou y participent en déterminent le ou les destinataires et qui ne comprend*

pas les services qui rendent possible une communication interpersonnelle et interactive uniquement en tant que fonction mineure accessoire intrinsèquement liée à un autre service ». La notion d'« opérateur » sera définie, après la transposition du CCEE dans la loi télécom, comme « *une personne ou entreprise qui fournit un réseau public de communications électroniques ou un service de communications électroniques accessible au public* ».

51. Ces modifications de définitions des concepts aboutissent à ce que les entreprises qui fournissent un service de communications électroniques « over-the-top », à l'instar, par exemple, de WhatsApp, Skype, Signal, ou encore Telegram, seront considérées comme des opérateurs soumis aux obligations de conservation des données de trafic et de localisation imposées par la loi télécom, telle qu'elle sera modifiée par l'avant-projet. **L'Autorité souligne que cette redéfinition des notions de « service de communications électroniques » et d'« opérateur » aboutit à étendre le champ d'application des dispositions autorisant ou imposant la conservation de telles données**.

2) Conservation des données à des fins de facturation et de paiement d'interconnexion (nouvel article 122 § 2 de la loi télécom)

52. Le nouvel article 122 § 2 de la loi télécom, qui transpose l'article 6 § 2 de la Directive ePrivacy, **autorise les opérateurs à conserver et traiter les données de trafic nécessaires pour établir les factures des abonnés ou effectuer les paiements d'interconnexion**. L'opérateur doit informer, avant le traitement, l'abonné ou, le cas échéant, l'utilisateur final auquel les données se rapportent, des types de données traitées, des objectifs précis du traitement et de la durée du traitement. Ce traitement de données est autorisé uniquement jusqu'à la fin de la période de contestation de la facture ou jusqu'à la fin de la période au cours de laquelle une action peut être menée pour en obtenir le paiement.

53. Les **traitement de données** autorisés par la nouvelle version de l'article 122 § 2 de la loi télécom **reposent sur une base juridique au sens de l'article 6.1 du RGPD** : l'exécution d'un contrat auquel la personne concernée est partie pour les traitements nécessaires pour établir les factures des abonnés (article 6.1.b) du RGPD) et la poursuite des intérêts légitimes du responsable du traitement ou d'un tiers pour les traitements nécessaires pour effectuer les paiements d'interconnexion (article 6.1.f) du RGPD).

54. Les **finalités poursuivies** – établir les factures des abonnés ou effectuer les paiements d'interconnexion – sont, conformément à l'exigence de l'article 5.1.b) du RGPD, **« *déterminées, explicites et légitimes* ».**

55. La nouvelle version de l'article 122 § 2 de la loi télécom n'identifie plus – contrairement à la version antérieure de l'article 122 § 2 de la loi télécom – les données précises qui peuvent être traitées sur pied de cette disposition. Si cette suppression aboutit à diminuer la prévisibilité de la norme autorisant le traitement de données, l'Autorité considère néanmoins qu'elle est admissible. En effet, la disposition indique que seules les données de trafic nécessaires pour établir les factures des abonnés ou effectuer les paiements d'interconnexion peuvent être traitées. Cette précision circonscrit de manière relativement prévisible les données qui peuvent être traitées[70]. En outre, l'Autorité comprend que les données de trafic nécessaires à ces fins peuvent varier selon les circonstances et qu'il est nécessaire que les opérateurs aient une marge de manœuvre à cet égard. Par ailleurs, il ressort de l'article 122 § 2 de la loi télécom que les personnes concernées doivent être informées, avant le traitement, des données qui seront traitées sur pied de cette disposition. Dans ces circonstances, l'Autorité considère que l'article 122 § 2 de la loi télécom reste suffisamment prévisible en ce qui concerne les catégories de données qui peuvent être traitées.

56. L'article 122 § 2 de la loi télécom, qui détermine **les critères permettant de déterminer la durée maximale de conservation**[71], **répond à l'exigence de l'article 5.1.e) du RGPD**.

3) Conservation des données pour assurer le marketing des services de communications électroniques propres et établir le profil d'utilisation ou des services à données de trafic ou de localisation (nouvel article 122 § 3 de la loi télécom)

57. **L'article 122 § 3 de la loi télécom**, qui transpose l'article 6.3 de la Directive ePrivacy, autorise les opérateurs à traiter et à conserver les données de trafic (qui incluent les données de localisation liées à une communication) nécessaires afin (i) d'assurer le **marketing** des services de communications électroniques propres et (ii) d'établir **le profil d'utilisation** de l'abonné ou de l'utilisateur final, **à condition d'avoir obtenu le consentement** de l'abonné ou, le cas échéant, de l'utilisateur final.

58. **Les modifications apportées par l'avant-projet de loi concernent la définition du « consentement »**. Cette notion est, à présent, définie par un renvoi à l'article 4 du RGPD (nouvel article 122 § 3, 2°, alinéa 2 de la loi télécom). Il s'ensuit que l'avant-projet prévoit que les abonnés ou utilisateurs finaux doivent avoir la possibilité de retirer leur consentement facilement et à tout moment (nouvel article 122 § 3, 3°). **L'Autorité prend note de ces changements** qui font suite à l'entrée en vigueur du RGPD.

[70] L'Autorité rappelle que les opérateurs, qui sont les responsables du traitement, devront respecter le principe de minimisation des données (article 5.1.c) du RGPD). Ainsi, si un abonné a un abonnement avec appels illimités, il n'apparait – à première vue – pas nécessaire de conserver les données de trafic permettant de comptabiliser le nombre ou la durée des appels sortants ayant été réalisé.

[71] L'Autorité constate, en outre, que les critères retenus par le législateur belge sont directement issus de la Directive ePrivacy.

59. L'avant-projet **remplace également la référence la loi du 8 décembre 1992** relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel **par une référence au RGPD et à la LTD**. L'Autorité **en prend note**.

4) Conservation des données pour détecter et analyser une fraude présumée ou une utilisation malveillante présumée d'un réseau de communications électroniques, en ce compris identifier son origine (nouvel article 122 § 4 de la loi télécom)

60. Le nouvel article 122 § 4 de la loi télécom **impose** aux opérateurs **de conserver des données de localisation et autres données de trafic nécessaires** afin de détecter et d'analyser **une fraude présumée** ou **une utilisation malveillante présumée** du réseau de communication électroniques.

61. La notion de « fraude » est définie par le nouvel article 122 § 4, alinéa 1er, de la loi télécom comme suit : « *un acte malhonnête fait dans l'intention de tromper en contrevenant à la loi, aux règlements ou au contrat et de se procurer ou de procurer à autrui un avantage illicite, commis par le biais de l'utilisation d'un service de communications électroniques* ».

62. La notion d'« utilisation malveillante du réseau » est définie par le nouvel article 122 § 4, alinéa 2, de la loi télécom comme suit : *« une utilisation du réseau afin d'importuner son correspondant ou de provoquer des dommages* ».

63. L'Exposé des motifs donne des exemples concrets de ce qui constitue une fraude ou une utilisation malveillante du réseau. Constituent une fraude, par exemple, le fait pour l'utilisateur final de ne pas respecter les conditions générales qui le lient à l'opérateur, le fait qu'un tiers fasse usage d'un service de communications électroniques au nom de l'abonné à son insu, le harponnage par SMS (« smishing »), le harponnage par Internet (« phishing ») ou encore un appel entrant induisant l'utilisateur final en erreur sur l'origine de cet appel et lui causant un préjudice (« spoofing »)[72]. L'utilisation malveillante du réseau couvre, par exemple, le harcèlement par téléphone[73].

64. Le nouvel article 122 § 4 de la loi télécom crée **une nouvelle obligation juridique** à charge des opérateurs de conserver et, le cas échéant de traiter, les données de localisation et autres données de trafic nécessaires afin de détecter et d'analyser une fraude présumée ou une utilisation malveillante présumée du réseau de communications électroniques. **Les traitements de données qui seront réalisés par les opérateurs sur pied de cette disposition seront, dès lors, « *nécessaires au***

[72] Exposé des motifs, p. 16.
[73] Exposé des motifs, p. 16.

respect d'une obligation légale à laquelle le responsable du traitement est soumis » (article 6.1.c) du RGPD).

65. Afin que ces traitements de données soient licites, il faut, comme le soulignait le Groupe de travail « Article 29 », que la loi remplisse « *toutes les conditions requises pour rendre l'obligation valable et contraignante, et [qu'elle soit] conforme au droit applicable en matière de protection des données, notamment aux principes de nécessité, de proportionnalité et de limitation de la finalité* »[74]. En d'autres termes, « ***le responsable du traitement ne doit pas avoir le choix de se conformer ou non à l'obligation*** »[75]. L'obligation légale doit être **claire et précise**, de telle sorte **que le responsable du traitement ne doit pas avoir de marge d'appréciation** quant à la façon de réaliser le traitement de données à caractère personnel nécessaire au respect de son obligation légale[76].

66. Le nouvel article 122 § 4 de la loi télécom **définit les finalités poursuivies par les nouveaux traitements de données qu'il impose** : il s'agit de détecter et d'analyser une fraude présumée ou une utilisation malveillante présumée d'un réseau de communications électroniques, en ce compris identifier son origine. L'Autorité constate que **ces finalités** sont, conformément à l'exigence de l'article 5.1.b) du RGPD, « ***déterminées, explicites et légitimes*** ». Par ailleurs, l'Autorité reconnait que ces finalités peuvent **répondre à l'un des objectifs listés par l'article 15 § 1 de la Directive ePrivacy**, en particulier la prévention, la recherche, la détection ou la poursuite d'infractions pénales et/ou la protection de la personne concernée ou des droits et libertés d'autrui[77]. **Il ne suffit toutefois pas que les objectifs** poursuivis par le nouvel article 122 § 4 de la loi télécom **soient légitimes pour que l'obligation de conservation des données qu'il impose soit admissible**. Il faut, en outre, **que cette obligation soit « rigoureusement »[78] nécessaire et proportionnée à ces objectifs**.

67. À ce propos, l'Autorité constate que le nouvel article 122 § 4 de la loi télécom **impose aux opérateurs de conserver de manière systématique des données** de localisation et d'autres données de trafic

[74] Groupe de travail « Article 29 », Avis *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*, p. 21.
[75] Groupe de travail « Article 29 », Avis *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*, p. 21.
[76] Groupe de travail « Article 29 », Avis *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*, p. 22.
[77] L'article 15 § 1 de la Directive ePrivacy liste plusieurs objectifs d'intérêt général permettant de justifier une limitation aux droits et obligations consacrés par les articles 5, 6 et 9 de ladite directive et fait, à la fin de cette liste, un renvoi à l'article 13 § 1 de la directive 95/46. Cette dernière disposition détermine les objectifs que peut poursuivre une mesure législative qui vise à limiter la portée des obligations et des droits prévus par la directive 95/46. Cette directive a été abrogée par l'article 94 du RGPD, lequel indique, en outre, que « *Les références faites à la directive abrogée s'entendent comme faites au présent règlement* ». Il s'ensuit que la référence faite à l'article 13 de la directive 95/46 doit être comprise comme une référence à l'article 23 du RGPD. L'article 23 du RGPD prévoit qu'une mesure législative peut limiter la portée des obligations et des droits prévus par le RGPD à condition qu'une *« telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir […] la protection de la personne concernée ou des droits et libertés d'autrui* ».
[78] Voyez le considérant 11 de la Directive ePrivacy

de l'ensemble des utilisateurs des moyens de communications électroniques[79]. Cette disposition constitue ainsi une **ingérence particulièrement grave** dans les droits au respect de la vie privée et à la protection des données à caractère personnel. **Le principe de proportionnalité exige que l'objectif d'intérêt général poursuivi par la mesure de conservation obligatoire soit en relation avec la gravité de l'ingérence qu'elle cause.** Or, la CJUE considère qu'une « *réglementation nationale prévoyant la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, en vue de lutter contre la criminalité grave, excède les limites du strict nécessaire et ne saurait être considérée comme étant justifiée dans une société démocratique* »[80]. **L'Autorité doute dès lors de la proportionnalité de l'obligation prévue par l'article 122 § 4 de la loi télécom au regard des objectifs qu'elle poursuit alors que ces objectifs, s'ils sont légitimes, ne semblent pas, à première vue, présenter le même degré d'importance que la lutte contre la criminalité grave**[81]. L'Autorité souligne, en outre, que l'avant-projet de loi prévoit que les différentes autorités identifiées par le nouvel article 127/1 de la loi télécom – dont « *les autorités compétentes pour la prévention, la recherche, la détection et la poursuite d'infractions pénales, d'infractions passibles d'une sanction administrative à caractère pénal, ou d'infractions commises à l'aide d'un réseau de communications électroniques, telles les infractions*

[79] À la suite d'une demande d'informations complémentaires, le délégué du Ministre conteste que l'article 122 § 4 de la loi télécom impose une conservation généralisée et indifférenciée des données de localisation et autres données de trafic en développant l'argumentation suivante (les notes de bas de pages ont été omises): *« Dans son arrêt 'La Quadrature du Net', la Cour de justice de l'Union européenne (CJUE) a précisé qu'une 'réglementation prévoyant la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation couvre les communications électroniques de la quasi-totalité de la population sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif poursuivi'. Or, le projet de loi soumis à l'avis de l'Autorité de protection des données effectue une différenciation au regard de l'objectif poursuivi, dès lors qu'il prévoit la conservation des seules données nécessaires au regard de chacune des finalités visées aux paragraphes 2, 3 et 4 de l'article 122 […]* ». Le délégué du demandeur considère ainsi que l'obligation de conservation n'est pas généralisée et indifférenciée parce qu'elle est imposée pour un objectif déterminé et que les données qui doivent être conservées sont les données nécessaires pour atteindre cette finalité. L'Autorité ne peut suivre cette argumentation. Le passage cité par le demandeur ne peut pas être coupé de son contexte et, en particulier, de la phrase qui le suit, laquelle indique qu'« *une telle réglementation […] concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, sans que ces personnes se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. Elle s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec cet objectif de lutte contre des actes de criminalité grave et, en particulier, sans que soit prévue une relation entre les données dont la conservation est prévue et une menace pour la sécurité publique* ». **Si on lit le § 143 de l'arrêt « Quadrature du Net » dans sa globalité, il ne peut être compris comme autorisant une conservation des données de trafic et de localisation de l'ensemble des utilisateurs d'un moyen de communication électronique dès lors que cette obligation poursuit un objectif déterminé et ne porte que sur des données de trafic nécessaires à cette fin.** Si tel avait été la position de la Cour, elle n'aurait pas exigé une conservation ciblée des données de trafic et de localisation aux fins de lutte contre la criminalité grave. **Le paragraphe 143 de l'arrêt du 6 octobre souligne qu'il doit exister un lien, même s'il peut être indirect ou lointain, entre les personnes dont les données seront conservées et l'objectif poursuivi par l'obligation de conservation**. L'obligation imposée par l'article 122 § 4 de la loi télécom porte sur les données de trafic et de localisation de tout utilisateur de moyens de communications électroniques sans qu'il soit requis qu'il existe un lien, même indirect et lointain, avec l'objectif de lutte contre la fraude ou l'utilisation malveillante du réseau. Certes, toute personne peut, potentiellement, commettre un « fraude » ou une « utilisation malveillante du réseau » ou, en être victime, mais cette potentialité – qui existe également pour les crimes graves dont la lutte constituait l'objectif de la règlementation sur laquelle portait l'arrêt de la CJUE – ne peut, au regard de la jurisprudence de la CJUE, être jugée suffisante pour justifier une conservation préventive systématique des données de trafic de l'ensemble des utilisateurs d'un moyen de communication électroniques nécessaires à la lutte contre la fraude et l'utilisation malveillante du réseau.

[80] CJUE, arrêt du 6 octobre 2020, § 141.

[81] À la suite d'une demande d'informations complémentaires, le délégué du Ministre semble reconnaitre, lui-même, que l'objectif de lutte contre la fraude et l'utilisation malveillante du réseau ne présente pas le même degré de gravité que la lutte contre la criminalité grave puisqu'il écrit « *L'article 127/1 s'inscrit pleinement dans cette jurisprudence européenne vu que le critère de proportionnalité est in concreto rencontré : en effet, si la conservation des données est justifiée originellement pour lutter, par exemple, contre les fraudes ou à des fins protection de la sécurité des réseaux, ces mêmes données peuvent a fortiori être traitées ultérieurement pour des finalités plus graves, à savoir, dans le cadre de la criminalité grave et de menace grave contre la sécurité publique* » (c'est l'Autorité qui souligne).

commises en ligne » – pourront avoir accès à ces données[82]. L'Autorité remarque qu'en imposant une nouvelle obligation de conservation généralisée des données de trafic et de localisation afin de lutter contre la fraude et l'utilisation malveillante du réseau tout en prévoyant, en parallèle, que les autorités répressives (entre autres) peuvent accéder à ces données, l'avant-projet de loi aboutit, *de facto*, à réintroduire une obligation de conservation généralisée et indifférenciée de ces données à des fins de lutte contre la criminalité. La CJUE a pourtant considéré qu'il n'était pas admissible d'imposer une telle obligation de conservation, et ce même pour lutter contre la criminalité grave, ce qui n'est pas le cas ici.

68. Par ailleurs, **l'Autorité s'interroge également sur la nécessité de l'obligation de conservation préventive et systématique des données qui est imposée par le nouvel article 122 § 4 de la loi télécom** à des fins de détection et d'analyse d'une fraude présumée ou d'une utilisation malveillante présumée du réseau de communication électroniques. **Ces objectifs ne pourraient-ils pas être atteints par des mesures moins intrusives dans les droits et libertés des personnes concernées ?** Ne serait-il pas possible, par exemple, de prévoir que l'obligation de conservation des données à des fins de lutte contre la fraude et l'utilisation malveillante du réseau peut être « activée » lorsqu'il existe des indices de fraude ou d'utilisation malveillante du réseau[83], auquel cas la conservation serait ciblée sur les personnes susceptibles d'être mêlées d'une manière ou d'une autre à la fraude ou à l'utilisation malveillante du réseau ou qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la lutte contre la criminalité grave ? Cette option rencontrerait l'exigence du « changement de perspective » mise en évidence par l'arrêt de la Cour constitutionnelle[84] : on passerait d'une conservation préventive et généralisée à une conservation réactive et ciblée. L'Autorité rappelle qu'il incombe au législateur de justifier que l'option qu'il choisit constitue la voie la moins attentatoire aux droits et libertés des personnes concernées pour atteindre l'objectif qu'il poursuit.

69. **L'Autorité invite dès lors le législateur à apprécier rigoureusement au regard de la jurisprudence de la CJUE, et à justifier, la mesure dans laquelle l'obligation de conserver les données de localisation et autres données de trafic nécessaires afin de détecter et d'analyser une fraude présumée ou une utilisation malveillante présumée du réseau de communication électroniques est effectivement nécessaire et proportionnée aux objectifs qu'elle poursuit**.

[82] Telle que cela ressort d'une lecture combinée des nouveaux articles 122 § 7 et 127/1 de la loi télécom
[83] L'indice d'une utilisation malveillante du réseau peut consister, par exemple, en une plainte faite par une personne qui s'estime victime de harcèlement. Le harcèlement étant, par définition, une infraction qui s'étale dans le temps, avec des occurrences répétitives, « activer » une obligation de conservation en cas de plainte permettrait probablement d'identifier la personne commettant le harcèlement. L'indice d'une fraude consistant à abuser des conditions générales de l'opérateur pourrait apparaitre en examinant les données conservées en vue de la facturation du service.
[84] C.C., arrêt du 21 avril 2021, § B.18.

70. Au-delà des interrogations fondamentales de l'Autorité concernant la nécessité et la proportionnalité de l'obligation imposée par le nouvel article 122 § 4 de la loi télécom, **l'Autorité a plusieurs remarques plus « ponctuelles » à formuler concernant la prévisibilité et la proportionnalité de certaines des modalités de cette obligation**.

71. Tout d'abord, **l'Autorité constate que cette disposition ne détermine pas avec précision les données qui doivent être conservées** en vue de détecter et d'analyser une fraude présumée ou une utilisation malveillante présumée du réseau de communication électroniques. Elle indique seulement que les opérateurs conservent « *les données de localisation et les autres données de trafic nécessaires à cette fin* » et qu'ils « *traitent les données de trafic nécessaires à cette fin, en ce compris lorsque c'est nécessaire, les données visées au paragraphe 2* [ndlr : les données de trafic nécessaires pour établir les factures des abonnés et les paiements d'interconnexion] ». L'article 122 § 4 de la loi télécom **contient une habilitation facultative au Roi** de déterminer les données de trafic qui doivent être conservées et traitées en application de cette disposition. Le Roi peut, mais ne doit pas, déterminer ces données[85].

72. L'Autorité rappelle, **qu'en vertu de l'exigence de prévisibilité**, **les données traitées doivent être déterminées par la règlementation qui encadre leur traitement**. Lorsque le traitement constitue une ingérence importante dans les droits et libertés des personnes concernées, comme c'est le cas en l'espèce, **le législateur doit déterminer, au moins, les catégories de données, étant donné que les données précises qui feront l'objet du traitement peuvent être définies dans une norme de rang règlementaire**. En l'espèce, il peut être admis **que le nouvel article 122 § 4 de la loi télécom définit suffisamment les catégories de données** qui doivent être conservées, à savoir « *les données de localisation et les autres données de trafic nécessaires [afin de détecter et d'analyser une fraude présumée ou une utilisation malveillante présumée d'un réseau de communications électroniques, en ce compris identifier son origine]* ». **La définition plus précise de ces données peut être déléguée au Roi, mais il est alors requis que le Roi intervienne**. Son intervention ne peut être facultative. En effet, tant que la règlementation ne comprend pas une définition plus précise des données à conserver, **l'exigence de prévisibilité n'est pas rencontrée**. Il en est d'autant plus ainsi que les notions de « fraude » et d'« utilisation malveillante du réseau » sont définies de manière assez large. Il est difficile dans ces circonstances pour les personnes concernées de prévoir quelles seront les données précises qui seront conservées en application de cette disposition. En outre, **lorsque le traitement est nécessaire au respect d'une obligation légale**, comme c'est le cas en l'espèce, il faut – comme l'Autorité l'a rappelé ci-dessus – que **tous les**

[85] L'Exposé des motifs justifie le caractère facultatif de cette habilitation législative comme suit : « *L'adoption de cet arrêté royal n'est pas obligatoire, au vu des défis suivants. D'abord, les fraudes évoluent significativement avec le temps. Certains types de fraude peuvent disparaître ou diminuer en importance alors que de nouveaux types de fraude peuvent voir le jour. Ensuite, les données que les opérateurs conservent pour lutter contre les fraudes peuvent être différentes selon le type de service de communications électroniques fourni, la taille de l'opérateur et les outils « anti-fraude » dont il dispose ou le type d'utilisateurs du service* ».

éléments qui permettent de circonscrire la portée de cette obligation soient déterminés par la norme imposant cette obligation, sans quoi le caractère contraignant de cette obligation pourra être remis en cause. Par ailleurs, et en tout état de cause, l'Autorité souligne que 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.

73. Ensuite, l'Autorité constate que le nouvel article 122 § 4 de la loi télécom impose aux opérateurs de conserver « *les données de localisation et les autres données de trafic nécessaires à cette fin, le temps nécessaire à cette fin et au minimum quatre mois* »[86], à l'exception **des données de trafic relatives aux communications entrantes dans le cadre de la fourniture de services de communications interpersonnelles qui doivent être conservées pendant 12 mois**. L'Autorité comprend que la possibilité de conserver les données de localisation et autres données de trafic au-delà du délai minimal de 4 mois vise la situation où une conservation plus longue est nécessaire pour gérer un contentieux relatif à une fraude ou à une utilisation malveillante du réseau. **Il convient d'ajouter cette précision dans l'avant-projet de loi.**

5) Conservation des données pour assurer la sécurité et le bon fonctionnement des réseaux et des services de communications électroniques, et en particulier pour détecter et analyser une atteinte potentielle ou réelle à cette sécurité, en ce compris identifier l'origine de cette atteinte (nouvel article 122 § 4/1 de la loi télécom)

74. Le **nouvel article 122 § 4/1** de la loi télécom **impose** aux opérateurs de **conserver** et de **traiter** les **données de trafic** nécessaires pour assurer **la sécurité et le bon fonctionnement de leurs réseaux et services de communications électroniques**, et en particulier pour détecter et analyser une atteinte potentielle ou réelle à cette sécurité, en ce compris identifier l'origine de cette atteinte.

[86] À la suite d'une demande d'informations complémentaires, le délégué du Ministre a justifié le choix de cette durée minimale de 4 mois comme suit : « *Comme indiqué par l'exposé des motifs, la durée minimale de 4 mois a été retenue pour la finalité de lutte contre la fraude et l'utilisation malveillante du réseau, étant donné que la fraude peut avoir un impact sur la facturation de l'opérateur envers l'abonné (ou d'une entreprise envers l'abonné). Tel est le cas, par exemple, lorsqu'un tiers fait usage d'un service de communications électroniques au nom de l'abonné à son insu. Dans ce cas, l'auteur de la fraude est un tiers et la victime l'utilisateur final qui se verra facturer par l'opérateur des communications non souhaitées. La durée minimale de 4 mois de conservation tient compte d'un cycle complet de facturation (premier mois suivant la consommation du service), d'une durée de contestation minimale (de 15 jours à 1 mois, le deuxième mois suivant la consommation du service), d'une période de traitement de la contestation permettant un échange entre l'abonné et l'opérateur (le troisième mois suivant la contestation du service) et d'une période de retard possible dans ce traitement (le quatrième mois suivant la consommation). Il s'agit par conséquent d'une estimation de la durée de conservation des données nécessaire, dans la majorité des cas, aux fins de lutte contre la fraude et l'utilisation malveillante du réseau. Néanmoins, cela ne constitue pas en soi une durée maximale de conservation afin de permettre à chaque opérateur de déterminer, pour ce qui le concerne, une durée de conservation plus longue et ce, en prenant en considération ses spécificités et nécessités particulières. La durée nécessaire peut en effet dépendre de multiples facteurs propres à chaque opérateur et sur lesquels ceux-ci doivent continuer à bénéficier d'une certaine liberté, par exemple quant au degré précis de protection contre la fraude qu'ils entendent fournir à leurs clients (et aux éventuels services additionnels à cet égard), à la méthodologie employée et aux ressources allouées à la détection des fraudes et utilisations malveillantes du réseau* ». L'Autorité souligne que les arguments avancés par le délégué du Ministre pour justifier une durée de conservation de 4 mois sont convaincants.

75. Le nouvel article 122 § 4/1 de la loi télécom crée ainsi **une nouvelle obligation juridique de conservation et de traitement de données de trafic** afin d'assurer la sécurité et le bon fonctionnement de leurs réseaux et services de communications électroniques. Ces traitements reposent sur une base juridique au sens de l'article 6 du RGPD puisqu'ils sont « *nécessaires au respect d'une obligation légale à laquelle le responsable du traitement est soumis* » (article 6.1.c) du RGPD). Comme l'Autorité l'a rappelé ci-dessus, la norme qui impose l'obligation légale doit être **suffisamment claire et précise** pour que le responsable du traitement n'ait pas de marge d'appréciation quant à la façon de s'y conformer[87].

76. Le nouvel article 122 § 4/1 de la loi télécom **définit la finalité poursuivie par les nouveaux traitements de données qu'il impose** : il s'agit d'« *assurer la sécurité et le bon fonctionnement de leurs réseaux et services de communications électroniques, et en particulier pour détecter et analyser une atteinte potentielle ou réelle à cette sécurité, en ce compris identifier l'origine de cette atteinte* ». L'Autorité constate que **cette finalité répond à l'exigence de l'article 5.1.b) du RGPD**. Par ailleurs, l'Autorité reconnait que cette finalité est comprise dans la liste des **objectifs** qui peuvent justifier, **aux termes de l'article 15 § 1 de la Directive ePrivacy**, une limitation de la portée de l'obligation de garantir la confidentialité des données de trafic. Il s'agit, en l'espèce, de « *la prévention, la recherche, la détection ou la poursuite d'utilisations non autorisées du système de communications électroniques* » [88] et/ou de la sauvegarde de la « sécurité publique »[89].

77. Comme l'Autorité l'a rappelé ci-dessus, **il ne suffit toutefois pas que l'obligation de conservation des données poursuivie un objectif légitime, mais il faut également que cette obligation soit « rigoureusement »[90] nécessaire et proportionnée à cet objectif**.

78. À ce propos, l'Autorité constate que le nouvel article 122 § 4/1 de la loi télécom – comme le nouvel article 122 § 4 de la loi télécom sur lequel l'Autorité s'est prononcée plus haut – **impose aux opérateurs de conserver de manière systématique des données de trafic de l'ensemble des utilisateurs des moyens de communications électroniques**. Cette nouvelle obligation de conservation préventive et généralisée constitue **une ingérence particulièrement grave** dans les droits et libertés des personnes concernées. L'Autorité rappelle, comme elle l'a déjà fait ci-dessus, qu'en vertu du principe de proportionnalité une ingérence grave dans les droits et libertés des

[87] Groupe de travail « Article 29 », Avis *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*, p. 22.
[88] Selon la CJUE, « l'exception visant les utilisations non autorisées du système de communications électroniques […] apparaît concerner les utilisations qui remettent en cause l'intégrité ou la sécurité même de ce système » (CJUE, arrêt di 29 janvier 2008, affaire C-275/06, « Promiscuae »)
[89] Selon l'Exposé des Motifs, « *la sécurité des réseaux, qui se rattache à la sécurité publique, est essentielle pour la société dans son ensemble. Un incident au niveau du réseau d'un opérateur peut avoir des conséquences très dommageables sur de nombreux plans (vol ou perte de données, impact sur tous les services qui sont offerts à l'aide du réseau). L'importance de la sécurité des réseaux va croître dans le futur avec le développement de la 5G, dont seront dépendants de nombreux services et applications* ».
[90] Voyez le considérant 11 de la Directive ePrivacy

personnes concernées ne peut être justifiée que par la poursuite d'un objectif d'intérêt général suffisamment important. Or, comme l'Autorité l'a déjà souligné plus haut, la CJUE considère qu'une « *réglementation nationale prévoyant la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, en vue de lutter contre la criminalité grave, excède les limites du strict nécessaire et ne saurait être considérée comme étant justifiée dans une société démocratique* »[91]. **L'Autorité doute dès lors de la proportionnalité de l'obligation prévue par l'article 122 § 4/1 de la loi télécom alors que l'objectif poursuivi par cette nouvelle obligation de conservation de données, s'il est légitime, ne semble pas, à première vue, présenter le même degré d'importance que la lutte contre la criminalité grave**. L'Autorité souligne, en outre, que l'avant-projet de loi prévoit que les différentes autorités identifiées par le nouvel article 127/1 de la loi télécom – dont « *les autorités compétentes pour la prévention, la recherche, la détection et la poursuite d'infractions pénales, d'infractions passibles d'une sanction administrative à caractère pénal, ou d'infractions commises à l'aide d'un réseau de communications électroniques, telles les infractions commises en ligne* » – pourront avoir accès à ces données[92]. Cette possibilité de permettre, notamment, aux autorités répressives d'avoir accès à toutes les données conservées par les opérateurs télécom en exécution de l'obligation qui leur est imposée par l'article 122 § 4/1 de la loi télécom renforce le doute de l'Autorité quant à la proportionnalité de cette obligation de conservation.

79. Par ailleurs, **l'Autorité s'interroge également sur la nécessité d'imposer une obligation de conservation préventive et systématique des données telle qu'elle est imposée par le nouvel article 122 § 4/1 de la loi télécom** afin d'assurer la sécurité et le bon fonctionnement de leurs réseaux et services de communications électroniques. Certes, les opérateurs doivent être en mesure de pouvoir traiter et conserver des données de trafic lorsque cela est nécessaire pour qu'ils puissent garantir la sécurité du réseau et de leurs services. **Mais l'Autorité se demande s'il est nécessaire de leur imposer une obligation de conservation des données à cette fin**. Actuellement, les opérateurs sont tenus par une obligation de prendre « *les mesures d'ordre technique et organisationnel appropriées pour gérer le risque en matière de sécurité des réseaux et des services de manière appropriée, le cas échéant conjointement en ce qui concerne la sécurité du réseau. Compte tenu des possibilités techniques les plus récentes, ces mesures garantissent un niveau de sécurité adapté aux risques existants. Des mesures sont notamment prises pour réduire au maximum les conséquences des incidents de sécurité pour les utilisateurs et les réseaux interconnectés* » (article 114 § 1 de la loi télécom[93]). Ils ont également la possibilité, « *dans le but exclusif de vérifier le bon fonctionnement du réseau et d'assurer la bonne exécution d'un service de communications électroniques* », d'identifier intentionnellement les personnes concernées par une transmission d'information et de prendre connaissance intentionnellement de données en matière de

[91] CJUE, arrêt du 6 octobre 2020, § 141.
[92] Telle que cela ressort d'une lecture combinée des nouveaux articles 122 § 7 et 127/1 de la loi télécom
[93] Cette disposition transpose l'article 4 de la Directive ePrivacy.

communications électroniques (articles 124 et 125 de la loi télécom). Si le bon fonctionnement du réseau et la bonne exécution d'un service de communications électroniques l'exigent, les opérateurs disposent déjà de la possibilité de traiter les données de trafic nécessaires à cette fin (et de les conserver le temps nécessaire à cette fin). **En transformant la possibilité de conserver et de traiter ces données en une obligation de les conserver, l'avant-projet crée une ingérence plus importante dans les droits et libertés des personnes concernées, concernées en particulier par rapport à des services qui, actuellement, ne collecte et ne conserve pas ces données pour des raisons de protection de la vie privée et de sécurité. L'aggravation de cette ingérence doit être justifiée de manière rigoureuse.** L'Exposé des motifs et les informations complémentaires fournies par le délégué du Ministre justifient pourquoi les opérateurs doivent pouvoir traiter des données de trafic pour assurer la sécurité du réseau et le bon fonctionnement de leurs services. **Mais la raison pour laquelle il est nécessaire de passer d'une possibilité à une obligation n'apparait pas suffisamment développée et étayée dans l'Exposé des motifs.**

80. **L'Autorité invite dès lors le législateur à apprécier rigoureusement au regard de la jurisprudence de la CJUE, et à justifier, la mesure dans laquelle l'obligation de conserver les données de trafic nécessaires afin d'assurer la sécurité et le bon fonctionnement de leurs réseaux et services de communications électroniques est effectivement nécessaire et proportionnée aux objectifs qu'elle poursuit**.

81. Au-delà des interrogations fondamentales de l'Autorité concernant la nécessité et la proportionnalité de l'obligation imposée par le nouvel article 122 § 4/1 de la loi télécom, **l'Autorité a plusieurs remarques plus « ponctuelles » à émettre concernant la prévisibilité et la proportionnalité de certaines des modalités de cette obligation**.

82. L'Autorité rappelle, **qu'en vertu de l'exigence de prévisibilité**, **les données traitées doivent être déterminées** par la règlementation qui encadre leur traitement, en particulier lorsque l'ingérence est particulièrement importante, comme c'est le cas en l'espèce. Or l'article 122 § 4/1 de la loi télécom **identifie la catégorie des données[94]** qui doivent être conservées, mais **il ne détermine pas les données précises** qui doivent être conservées. Il n'habilite pas, non plus, le Roi à procéder à cette détermination. **L'exigence de prévisibilité n'est dès lors pas rencontrée**. L'avant-projet doit **soit déterminer lui-même** les données précises qui doivent être conservées, **soit déléguer au Roi** le soin de procéder à cette détermination[95]. En tout état de cause, l'Autorité souligne que la conservation

[94] Il s'agit des « *données de trafic qui sont nécessaires pour assurer la sécurité et le bon fonctionnement de leurs réseaux et services de communications électroniques, et en particulier pour détecter et analyser une atteinte potentielle ou réelle à cette sécurité, en ce compris l'origine de cette atteinte* »

[95] Comme l'Autorité l'a déjà souligné, cette exigence de précision est également imposée par le fait que la conservation de ces données repose sur « une obligation légale » (au sens de l'article 6.1.c) du RGPD). Or, dans une telle situation, tous les éléments

des données de trafic ne doit pas contenir ou permettre de déduire l'url spécifique des pages web visitées par les personnes concernées.

83. Ensuite, l'Autorité constate que le nouvel article 122 § 4/1 de la loi télécom **impose une durée de conservation de 12 mois,** étant entendu que les opérateurs « *peuvent **les conserver pour une durée plus longue, qui est limitée au strict nécessaire*** ». L'Autorité a **deux remarques** à formuler à ce propos.

(i) **Premièrement**, l'Autorité **s'interroge sur la proportionnalité de la durée de conservation de 12 mois**. L'Autorité se demande, en particulier, s'il ne pourrait pas être suffisant de conserver les données pendant un laps de temps plus court, en donnant la possibilité de prolonger cette durée uniquement si l'opérateur constate une atteinte à la sécurité ou au bon fonctionnement du réseau ou des services de communications électroniques ? **L'Autorité invite le législateur à apprécier, et, le cas échéant, à justifier à l'aide d'éléments concrets, la raison pour laquelle les données doivent être conservées pendant une durée de 12 mois**. Lors de cet exercice, le législateur doit prendre en compte le fait qu'aux termes de la loi télécom les opérateurs doivent veiller à être en mesure de détecter rapidement une atteinte à la sécurité des réseaux ou des services qu'ils fournissent.

(ii) **Deuxièmement,** l'Autorité note que le législateur entend permettre de prolonger la durée de conservation de 12 mois si cela est strictement nécessaire. L'Autorité comprend que cette possibilité vise la situation où une conservation plus longue de certaines données de trafic ou de localisation est nécessaire pour gérer un contentieux relatif à une attaque ou des actes portant atteinte à la sécurité du réseau ou au bon fonctionnement du service, étant entendu que seules les données nécessaires à la gestion du contentieux peuvent être conservées pour une durée plus longue. **Cette précision sera ajoutée à l'avant-projet.**

6) Conservation des données pour répondre à une obligation légale (nouvel article 122 § 4/2 de la loi télécom)

84. Le **nouvel article 122 § 4/2** de la loi télécom **impose** aux opérateurs de **conserver** et de **traiter** les **données de trafic** nécessaires **pour répondre à une obligation légale dans leur chef**, pour la durée nécessaire à cette fin.

qui permettent de circonscrire la portée de cette obligation – y compris donc les données à conserver – doivent être déterminés par la norme imposant cette obligation, sans quoi le caractère contraignant de cette obligation pourra être remis en cause.

85. **L'avant-projet doit préciser que cette obligation légale ne peut être imposée que par une norme législative formelle**. En effet, au vu de la gravité de l'ingérence causée par la conservation de données de trafic, il est requis que toute obligation de conservation de données soit imposée par une norme législative formelle qui en détermine, d'une manière prévisible, tous les éléments essentiels. À toutes fins utiles, l'Autorité souligne encore que cette norme législative devra également respecter les principes de nécessité et de proportionnalité, tels qu'ils sont interprétés par la CJUE.

7) Conservation des données de localisation autres que les données de trafic (nouvel article 123 de la loi télécom)

86. Le nouvel article 123 § 1 de la loi télécom **autorise** les **opérateurs de réseaux mobiles** à traiter et à conserver **des données de localisation autres que des données de trafic** dans les cas suivants :

- Lorsque cela **est nécessaire pour le bon fonctionnement et la sécurité du réseau ou du service**, les données étant conservées le temps nécessaire à cette fin ;

- Lorsque cela est **nécessaire pour détecter ou analyser les fraudes ou l'utilisation malveillante du réseau**, les données étant conservées le temps nécessaire à cette fin ;

- Lorsque **les données ont été rendues anonymes** ;

- Lorsque **le traitement s'inscrit dans le cadre de la fourniture d'un service à données de trafic ou de localisation** et que l'abonné ou, le cas échéant, l'utilisateur final, **y a donné son consentement** ;

- Lorsque **le traitement est nécessaire pour répondre à une obligation légale** dans le chef de l'opérateur.

87. Bien que l'Exposé des motifs indique que l'article 123 de la loi télécom transpose l'article 9 de la Directive ePrivacy, **l'Autorité constate que les situations dans lesquelles cette disposition autorise une conservation des données de localisation autres que des données de trafic sont plus nombreuses que celles qui sont mentionnées par l'article 9 de la Directive ePrivacy**. En effet, l'article 9 de la Directive ePrivacy n'autorise un traitement des données de localisation autres que des données de trafic uniquement après qu'elles aient été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés, dans la mesure et pour la durée

nécessaire à la fourniture d'un service à valeur ajoutée. L'article 9 de la Directive ePrivacy ne prévoit pas le traitement et la conservation des données de localisation autres que les données de trafic qui sont nécessaires pour le bon fonctionnement et la sécurité du réseau ou du service, pour détecter ou analyser les fraudes ou l'utilisation malveillante du réseau ou pour répondre à une obligation légale dans le chef de l'opérateur. Toutefois, l'article 15 § 1 de la Directive ePrivacy autorise « [*l]es États membres [à] adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus […] à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale — c'est-à-dire la sûreté de l'État — la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe* ». **Le législateur belge peut donc prévoir le traitement et la conservation de données de localisation autres que des données de trafic dans d'autres situations que celles prévues par l'article 9 de la Directive ePrivacy**, **<u>à condition</u>** que ces traitements **soient « nécessaires » et « proportionnés »** au regard de(s) (l') objectif(s) qu'ils poursuivent **et que la disposition légale qui les prévoit soit suffisamment prévisible** pour les personnes concernées.

88. À ce propos, l'Autorité constate **que l'Exposé des motifs ne justifie ni la nécessité ni la proportionnalité** des traitements de données de localisation autres que des données de trafic afin d'assurer **le bon fonctionnement et la sécurité du réseau ou du service**, ou afin de détecter ou analyser **les fraudes ou l'utilisation malveillante du réseau**[96]. L'Autorité invite dès lors le **législateur à apprécier rigoureusement, et le cas échéant à justifier à l'aide d'éléments concrets, la nécessité et la proportionnalité de ces traitements**. Par ailleurs, **afin de rencontrer l'exigence de prévisibilité**, l'avant-projet devra être revu afin de **déterminer**, au moins, les **conditions dans lesquelles les opérateurs pourront conserver et traiter ces données** et **les durées maximales de conservation** de ces données.

89. Concernant les traitements des données de localisation autres que des données de trafic **nécessaires au respect d'une obligation légale dans le chef de l'opérateur**, l'Autorité souligne que l**'avant-projet doit préciser –** au vu de la gravité de l'ingérence causée par la conservation de données de localisation – **que cette obligation légale ne peut être imposée que par une norme législative formelle**. À toutes fins utiles, l'Autorité souligne encore que cette norme législative devra également respecter les principes de nécessité et de proportionnalité, tels qu'ils sont interprétés par la CJUE.

[96] Concernant les objectifs poursuivis par ces traitements de données, l'Autorité a déjà pu souligner que ceux-ci répondaient à l'exigence de l'article 5.1.b) du RGPD et qu'ils étaient compris dans la liste des objectifs de l'article 15 § 1 de la Directive ePrivacy

90. Enfin, l'Autorité souligne que les données de localisation ne peuvent être que très difficilement rendues réellement anonymes lorsqu'elles sont conservées à un niveau individuel[97]. En effet, les opérateurs qui ont accès à des données de localisation qui se rattachent à une personne physique identifiée (et qui n'ont donc pas encore été rendues anonymes) peuvent aisément utiliser ces informations afin d'identifier, à travers des « *profiling attacks* »[98], les personnes auxquelles se rattachent les données de localisation qui ont été « anonymisées ».

8) Conservation des données de souscription et des données techniques permettant d'identifier l'utilisateur final, l'équipement terminal ou le service de communications électroniques employé (nouvel article 126 de la loi télécom) et des données d'identification des abonnés (nouvel article 127 de la loi télécom)

91. Le nouvel article 126 de la loi télécom **impose** aux « *opérateurs qui offrent aux utilisateurs finaux des services de communications électroniques* » ainsi qu'aux « *opérateurs fournissant les réseaux de communications électroniques sous-jacents* » 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 communication électronique employé, pour autant que ces opérateurs traitent ou génèrent déjà ces données dans le cadre de la fourniture des réseaux ou services de communication concernés**. Ces données, à l'exception des adresses IP dynamiques autres que celle qui a été utilisée pour souscrire au service, doivent être conservées à partir de la date d'activation du service et jusqu'à 12 mois après la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé. Les adresses IP dynamiques autres que celle qui a été utilisée pour souscrire au service sont, pour leur part, conservées pendant 12 mois après la fin de la session.

92. Le nouvel article 126 § 2 **délègue au Roi** le soin de **déterminer les données à conserver** ainsi que les exigences auxquelles ces données doivent répondre. **L'arrêté du 19 septembre 2013**, que le projet d'arrêté soumis pour avis à l'Autorité modifie**, détermine la liste des données qui doivent être conservées** en exécution de l'article 126 de la loi télécom :

- Les fournisseurs **de services de téléphonie fixe accessibles au public**, en ce compris les services nomades, et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

[97] Des données sont conservées à un niveau individuel lorsque les informations enregistrées sont liées à une personne. Au contraire, les informations, qui sont enregistrées de manière agrégée, ne contiennent que des informations liées à plusieurs personnes, par exemple, un pourcentage.
[98] Voyez, par exemple, Naini, F.M., Unnikrishnan, J., Thiran, P. and Vetterli, M., 2015. "Where you are is who you are: User identification by matching statistics". *IEEE Transactions on Information Forensics and Security*, 11(2), pp.358-372.

1° le numéro attribué à l'utilisateur final ;
2° les données personnelles de l'utilisateur final (qui sont définies comme « *les nom et prénom ainsi que les adresses de facturation et de livraison de l'utilisateur final* ») ;
3° la date de début de l'abonnement ou de l'enregistrement au service ;
4° le type de service de téléphonie fixe utilisé ainsi que les services annexes auxquels l'utilisateur final a souscrit ;
5° en cas de transfert du numéro de l'utilisateur final auprès d'un autre fournisseur, l'identité du fournisseur qui transfère le numéro et l'identité du fournisseur auquel le numéro est transféré ;
6° les données relatives au type de paiement, à l'identification du moyen de paiement et à la date du paiement de l'abonnement ou de l'utilisation du service ;
7° le numéro d'identification du terminal de l'utilisateur final, le cas échéant l'adresse « MAC (Media Access Control) » ou le « PEI (Permanent Equipment Identifier) ».

- Les fournisseurs d'un **service de téléphonie mobile accessible au public**, en ce compris les services nomades, et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

  1° le numéro attribué à l'utilisateur final ainsi que l'identité internationale d'abonné mobile (« International Mobile Subscriber Identity », IMSI ») ou « Subscription Permanent Identifier (SUPI) ») ;
  2° les données personnelles de l'utilisateur final et le « Subscription Concealed Identifier (SUCI) » correspondant ;
  3° la date et le lieu de la souscription à l'abonnement ou de l'enregistrement de l'utilisateur final ;
  4° la date et l'heure de la première activation du service, ainsi que l'identifiant cellulaire à partir duquel le service a été activé ;
  5° les services annexes auxquels l'utilisateur final a souscrit ;
  6° en cas de transfert de numéro auprès d'un autre opérateur, l'identité de l'opérateur d'origine de l'utilisateur final ;
  7° les données relatives au type de paiement, à l'identification du moyen de paiement et à la date du paiement de l'abonnement ou de l'utilisation du service ;
  8° le numéro d'identification du terminal de l'utilisateur final (« International Mobile Equipment Identity », « IMEI », l'adresse « MAC (Media Access Control) » ou « Permanent Equipment Identifier (PEI) »).

- Les fournisseurs de service **d'accès à l'internet** accessible au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

  1° l'identifiant de l'utilisateur final, en ce compris le cas échéant le « Subscription Permanent Identifier (SUPI) » ;
  2° a) l'adresse IP ;
  b) en cas d'utilisation partagée d'une adresse IP, les ports attribués de l'adresse IP ainsi que la date et l'heure de l'attribution ;
  3° les données personnelles de l'utilisateur final, en ce compris le cas échéant le « Subscription Concealed Identifier (SUCI) » correspondant ;
  4° la date et l'heure de la souscription à l'abonnement ou de l'enregistrement de l'utilisateur final ;
  5° l'adresse IP et le port source de la connexion ayant servi à la création de l'abonnement ou à l'enregistrement de l'utilisateur final ;
  6° l'identification du point de terminaison du réseau ayant servi à la création de l'abonnement ou de l'inscription en tant qu'utilisateur final ;
  7° les services annexes auxquels l'utilisateur final a souscrit auprès du prestataire d'accès Internet public concerné ;
  8° les données relatives au type de paiement, à l'identification du moyen de paiement et à la date du paiement de l'abonnement ou de l'utilisation du service ;
  9° le numéro d'identification du terminal de l'utilisateur final, le cas échéant l'adresse « MAC (Media Access Control) » ou le « PEI (Permanent Equipment Identifier) ».

- Les fournisseurs d'un **service de courrier électronique par internet accessible au public,** les fournisseurs d'un **service de téléphonie par internet accessible au public** et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

  1° l'identifiant de l'utilisateur final, en ce compris le cas échéant le « Subscription Permanent Identifier (SUPI) »
  2° l'adresse IP et le port source utilisés par l'utilisateur final ;
  3° les données personnelles de l'utilisateur final, en ce compris le cas échéant le « Subscription Concealed Identifier (SUCI) » correspondant ;
  4° la date et l'heure de la création du compte de courrier électronique ou de téléphonie par internet ;
  5° l'adresse IP et le port source ayant servi à la création du compte de courrier électronique ou de téléphonie par l'internet ;

6° les données relatives au type de paiement, à l'identification du moyen de paiement et à la date du paiement de l'abonnement ou de l'utilisation du service ;
7° sauf pour le service de courrier électronique par internet accessible au public, le numéro d'identification du terminal de l'utilisateur final, le cas échéant l'adresse « MAC (Media Access Control) » ou le « PEI (Permanent Equipment Identifier) ».

93. Le nouvel **article 127** de la loi télécom **impose**, pour sa part, aux opérateurs **d'identifier leurs abonnés** ou de collecter et conserver les données nécessaires, y compris, le cas échéant le numéro de registre national, pour que les autorités qui sont habilitées à obtenir cette identité puissent les identifier. Ces données doivent être **conservées pendant toute la durée d'activation** du service **et jusqu'à douze mois après la date à partir de laquelle une communication est possible pour la dernière fois** à l'aide du service utilisé. **Le Roi** est habilité – mais sans y être tenu – **à déterminer**, entre autres, **les données** et documents d'identification à collecter et à conserver par l'opérateur.

94. Les **données conservées en exécution des articles 126 et 127** de la loi télécom le sont **pour les autorités et les finalités suivantes** :

« *1° les autorités compétentes pour la prévention, la recherche, la détection et la poursuite d'infractions pénales, d'infractions passibles d'une sanction administrative à caractère pénal, ou d'infractions commises à l'aide d'un réseau de communications électroniques, telles les infractions commises en ligne ;*
2° 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 ;
3° les autorités chargées d'apporter de l'aide aux personnes, en ce compris le service de médiation pour les télécommunications pour ce qui concerne l'utilisation malveillante du réseau, les services d'urgence et la Cellule des personnes disparues de la Police Fédérale ;
4° l'Institut dans le cadre de la mise en œuvre et le contrôle de la présente loi ;
5° les autorités compétentes pour l'examen d'une défaillance de la sécurité du réseau ou du service »[99].

95. Il ressort de la jurisprudence de la Cour de **justice qu'une mesure législative prise en application de l'article 15 de la Directive ePrivacy peut imposer aux opérateurs de conserver les données nécessaires à l'identification des utilisateurs d'un service de communications électroniques** si cette conservation s'avère nécessaire à la poursuite de l'un des objectifs énoncés par l'article 15.1 de la Directive ePrivacy.

[99] Nouvel article 127/1 de la loi télécom

96. Concernant **les données portant sur l'identité civile des abonnés**, la CJUE estime que leur conservation – sans délai particulier – et leur communication à la seule fin de l'identification de l'utilisateur concerné peut être justifiée par la poursuite de l'un des objectifs listés à l'article 15 § 1 de la Directive ePrivacy sans qu'il soit nécessaire que cet objectif revête une importance particulière (comme, par exemple, la lutte contre la criminalité grave). **La conservation des données relatives à l'identité civile des abonnés** afin de permettre leur identification **ne constitue pas**, aux yeux de la Cour, **une ingérence grave** dans les droits fondamentaux des personnes concernées.

97. En revanche, la Cour procède à une **appréciation plus stricte concernant la conservation de l'adresse IP des abonnés**. Cette donnée, qui est nécessaire à l'identification de la personne physique propriétaire d'un équipement terminal à partir duquel une communication au moyen de l'Internet est effectuée, permet également – si elle combinée aux adresses IP destinataires – d'effectuer un traçage exhaustif du parcours de navigation de l'internaute et ainsi d'établir son profil détaillé. La Cour estime dès lors **que la conservation généralisée des adresses IP attribuées à la source d'une connexion constitue une ingérence grave** dans les droits fondamentaux des internautes. Elle admet néanmoins qu'une telle conservation préventive généralisée puisse s'avérer nécessaire parce que, dans le cas d'une infraction commise en ligne, l'adresse IP peut constituer le seul moyen d'investigation permettant l'identification de la personne à laquelle cette adresse était attribuée au moment de la commission de cette infraction. Toutefois, eu égard à la gravité de l'ingérence, la Cour estime que **seul un objectif suffisamment important, à l'instar de la lutte contre la criminalité grave, peut justifier une telle mesure de conservation généralisée des adresses IP**[100].

98. L'Autorité prend note de la volonté du législateur d'imposer la conservation des données de souscription et d'identification des abonnés ainsi que des données techniques permettant leur identification, l'identification de l'équipement terminal utilisé et du service de communications électroniques utilisé. **Une telle conservation des données peut, en effet, s'avérer, à certaines conditions, nécessaire et proportionnée aux objectifs qu'elle poursuit**.

99. Toutefois, l'Autorité souligne que le niveau d'ingérence causé par la conservation de ces données varie selon le type de donnée sur laquelle elle porte. La conservation **des données qui permettent un traçage des activités des abonnés** constitue une **ingérence grave** dans les droits fondamentaux des personnes concernées alors que la conservation des données qui identifient les abonnés sans permettre le traçage de leur activité constitue une ingérence dans leur vie privée qui ne doit pas être qualifiée de grave. L'Autorité rappelle que le **principe de proportionnalité exige que la conservation des données qui permettent un traçage des activités des abonnés,** pour d'autres finalités que l'acheminement de la communication électronique **et leur utilisation**

[100] CJUE, arrêt du 6 octobre 2020, § 156

ultérieure éventuelle pour les motifs énoncés à l'articles 15 de la Directive ePrivacy **soient soumises à des conditions plus strictes afin que l'ingérence qu'elles créent reste strictement proportionnée aux objectifs poursuivis.**

100. Concernant **les adresses IP attribuées à la source d'une communication**, la CJUE estime que leur conservation ne peut avoir lieu qu'en vue de la poursuite d'objectifs suffisamment importants, que la durée de leur conservation doit être limitée au strict nécessaire au regard de ces objectifs et qu'il doit exister conditions et garanties strictes quant à l'exploitation de ces données[101]. **L'avant-projet devra dès lors être revu afin de prévoir que les adresses IP attribuées à la source d'une connexion ne pourront être conservées qu'afin de permettre la poursuite d'objectifs particulièrement importants qui devront y être précisés**.

101. L'Autorité constate, en outre, que **ni l'avant-projet de loi ni le projet d'arrêté ne précisent que seules les adresses IP attribuées à la source d'une communication doivent être conservées en exécution du nouvel article 126 de la loi télécom**, à l'exclusion des adresses IP du destinataire de cette communication. **L'avant-projet de loi et le projet d'arrêté seront revus afin d'ajouter cette précision**.

102. L'avant-projet de loi – et le projet d'arrêté qui l'exécute – **prévoient également la conservation des numéros d'identification des terminaux des utilisateurs finaux.** Sauf erreur, l'exigence de conservation de cette donnée est nouvelle. 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. **La conservation préventive et systématique de ces numéros constitue dès lors une ingérence importante dans les droits au respect de la vie privée et à la protection des données à caractère personnel**. Leur conservation doit dès lors être soumise **au strict respect des conditions de nécessité et de proportionnalité** au regard des objectifs poursuivis. À cet égard, la jurisprudence de la Cour de Luxembourg concernant la conservation généralisée des adresses IP peut être utilement mobilisée pour déterminer les conditions que doit rencontrer une mesure législative qui impose la conservation de telles données d'identification unique des équipements terminaux des abonnés. Le délégué du Ministre, dans une réponse à une demande d'informations complémentaires, souligne d'ailleurs, lui aussi, que le raisonnement suivi par la CJUE à propos des adresses IP « *peut être suivi quant aux autres données techniques nécessaires pour identifier l'utilisateur final, l'équipement terminal, le service de communication électroniques employé* ». **Ainsi, la conservation de ces données ne devrait être imposée qu'afin de poursuivre un objectif présentant une**

[101] CJUE, arrêt du 6 octobre 2020, § 156. Certes, ces exigences portent sur la conservation généralisée et indifférenciée des adresses IP et non de toutes données techniques permettant l'identification de l'abonné ou de son équipement terminal, mais comme le délégué du Ministre l'a indiqué lui-même, dans une réponse à une demande d'informations complémentaires, « *Le même raisonnement peut être suivi quant aux autres données techniques nécessaires pour identifier utilisateur final, l'équipement terminal, le services de communication électroniques employé* ».

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**[102]. **L'avant-projet de loi et le projet d'arrêté**, qui ne rencontrent pas ces exigences, **devront donc être adaptés afin d'y répondre.**

103. Au-delà de ces remarques portant sur le principe des obligations de conservation des données de souscription et d'identification des abonnés ainsi que des données techniques permettant leur identification, l'identification de l'équipement terminal utilisé et du service de communications électroniques utilisé, l'Autorité a **deux remarques plus ponctuelles** à émettre relativement aux différentes dispositions qui encadrent ces obligations de conservation.

104. Premièrement, l'Autorité constate que le **nouvel article 127 § 2** de la loi télécom **entend permettre l'utilisation d'une technologie de reconnaissance faciale** à des fins d'identification de l'abonné**. 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. Cette possibilité **d'utiliser la reconnaissance faciale** comme moyen d'identification sera dès lors supprimée de l'avant-projet de loi. L'Autorité souligne, en outre**, que l'utilisation d'autres données biométriques, à l'instar des empreintes digitales, excèderait également ce qui est nécessaire et admissible dans une société démocratique**.

105. Ensuite, le **nouvel article 127 § 3** de la loi télécom habilite le Roi, **mais de manière facultative**, à déterminer les données et documents d'identification à collecter et à conserver par l'opérateur. L'exigence de prévisibilité requiert que ces données et documents soient déterminés. **Soit le législateur procède lui-même à cette détermination, soit il délègue au Roi le soin d'y procéder, mais** cette **habilitation** doit alors présenter un caractère **obligatoire**. **L'avant-projet de loi sera revu en ce sens.**

[102] CJUE, arrêt du 6 octobre 2020, § 156.

9) Conservation ciblée des données de trafic et de localisation 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 (nouvel article 126/1 de la loi télécom)

106. Le nouvel article 126/1 de la loi télécom **impose** aux opérateurs de conserver, en principe, **pendant 12 mois**[103], les **données de trafic et de localisation** de **toutes les communications** effectuées **à partir**, ou **vers**, une des **zones géographiques** qu'il liste. L'avant-projet de loi précise toutefois que les opérateurs ne doivent conserver ces données que s'ils 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[104]. 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**. Une telle **obligation de conservation ciblée** est, **dans son principe**, **conforme aux exigences européennes** telle qu'interprétées par la CJUE.

107. L'Autorité constate toutefois que **le nouvel article 126/1 de la loi télécom appelle plusieurs commentaires** au regard des principes fondamentaux de la protection des données.

- ***Commentaires portant sur le nouvel article 126/1 § 2 de la loi télécom :***

108. Le nouvel article 126/1 § 2 de la loi télécom **détermine les catégories de données** qui doivent être conservées par les opérateurs. Il s'agit des données suivantes :

> « *1° les données relatives à l'accès et la connexion de l'équipement terminal au réseau et au service et à la localisation de cet équipement, y compris le point de terminaison du réseau ;*

[103] 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.
[104] 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 ».

2° les données de communication, à l'exclusion du contenu, en ce compris leur origine et leur destination ;
3° les données des appels infructueux, pour autant que ces données soient, dans le cadre de la fourniture des services de communications concernés :
i° en ce qui concerne les données de la téléphonie, générées ou traitées par les opérateurs ; ou
ii° en ce qui concerne les données de l'internet, journalisées par ces opérateurs.

Le Roi fixe, par arrêté délibéré en Conseil des ministres, sur proposition du ministre et du ministre de la Justice, du ministre de l'Intérieur, du ministre de la défense, et du ministre, après avis des Autorités de protection des données compétentes et de l'Institut, les données à conserver et peut fixer les exigences auxquelles ces données doivent répondre »

109. Tout d'abord, l'Autorité constate **que le nouvel article 126/1 § 2 de la loi télécom utilise le concept de « *données de communication* »** pour déterminer les catégories de données qui doivent être conservées alors que les autres dispositions de la loi télécom qui autorisent ou imposent une conservation des données utilisent, pour leur part, les concepts de « *données de trafic* », « *données de localisation* » ou « *données de localisation autres que les données de trafic* ». Ces trois dernières catégories de données sont définies, directement ou indirectement, par la loi télécom ; ce qui n'est pas le cas pour la notion de « données de communication ». **Cette absence de définition nuit à la prévisibilité de la loi**. Il en est d'autant plus ainsi que l'utilisation d'un concept différent pour identifier les données qui doivent être conservées en vertu du nouvel article 126/1 de la loi télécom laisse supposer que la notion de « données de communication » viserait d'autres types de données que les « données de trafic » et « les données de localisation ». À la suite d'une demande d'informations complémentaires, le délégué du Ministre a indiqué que « *La notion de données de communication est un sous-ensemble de la notion de trafic. Il s'agit de données qui donne des informations sur l'auteur ou le destinataire de la communication (qui a contacté qui/quoi)* ». **Afin de respecter l'exigence de prévisibilité**, **l'avant-projet de loi doit être revu afin d'y définir la notion de « données de communication »**.

110. Ensuite, **une même remarque doit être formulée à propos de la notion « données des appels infructueux »**. En effet, bien que la notion d'« appels infructueux » soit définie dans la loi télécom[105], la notion de « données des appels infructueux » ne l'est pas. À la suite d'une demande d'informations complémentaires, le délégué du Ministre a indiqué que « *Les 'données des appels infructueux' visent les données de trafic liées aux appels infructueux. Il peut s'agir,*

[105] Cette notion est définie par l'article 2 de l'avant-projet de loi qui insère un 74° à l'article 2 de la loi télécom : « toute communication au cours de laquelle un appel a été transmis mais est resté sans réponse ou a fait l'objet d'une intervention de la part du gestionnaire du réseau ».

par exemple, de la date et heure de cet appel et du numéro de l'appelant ». **Afin de répondre à l'exigence de prévisibilité de la loi, l'avant-projet de loi doit être revu afin d'y inscrire cette précision : la notion de « données des appels infructueux » sera remplacée par la notion de « données de trafic des appels infructueux ».**

111. Le nouvel article 126/1 § 2 **délègue au Roi** le soin de déterminer les données à conserver. Cette habilitation est « obligatoire » puisque le Roi est tenu de fixer les données à conserver. **L'Autorité estime qu'une telle délégation au Roi est admissible au regard du principe de légalité** : les catégories de données sont définies avec suffisamment de précision dans la loi (à condition toutefois que l'avant-projet de loi soit modifié pour répondre aux remarques émises par l'Autorité dans les paragraphes précédents) et la matière présente une technicité qui justifie de déléguer au Roi le soin de déterminer les données de trafic précises qui doivent être conservées.

112. **L'arrêté royal du 19 septembre 2013,** qui est modifié par le projet d'arrêté soumis pour avis à l'Autorité, **exécute le nouvel article 126/1 § 2 de la loi télécom** et fixe les données que les opérateurs doivent conserver en exécution de cette disposition :

- Les fournisseurs **de services de téléphonie fixe accessibles au public**, en ce compris les services nomades, et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent, « **au minimum** », les données suivantes :

  1° l'identification du numéro de téléphone de l'appelant et de l'appelé ;
  2° la localisation du point de terminaison du réseau de l'appelant et de l'appelé
  3° en cas d'appel multiple, de déviation ou de renvoi, l'identification de toutes les lignes en ce compris, celles vers lesquelles l'appel a été transféré ;
  4° la date et l'heure exacte du début et de la fin de l'appel ;
  5° la description du service de téléphonie utilisé.

- Les fournisseurs d'un **service de téléphonie mobile accessible au public**, en ce compris les services nomades, et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent, « **au minimum** » les données suivantes :

  1° l'identification du numéro de téléphone de l'appelant et de l'appelé ;
  2° en cas d'appel multiple, de déviation ou de renvoi, l'identification de toutes les lignes en ce compris, celles vers lesquelles l'appel a été transféré ;

3° l'identité internationale d'abonné mobile (« International Mobile Subscriber Identity », « IMSI ») ou « Subscription Permanent Identifier » (SUPI) de l'appelant et de l'appelé
4° l'identité internationale d'équipement mobile (« International Mobile Equipment Identity », « IMEI ») ou « Permanent Equipment Identifier (PEI) » du terminal mobile de l'appelant et de l'appelé ;
5° la date et l'heure exacte du début et de la fin de l'appel ;
6° la localisation du point de terminaison du réseau au début et à la fin de chaque connexion ;
7° les données permettant d'établir la localisation géographique des cellules en se référant à leur identifiant cellulaire au moment où la communication a été effectuée
8° les caractéristiques techniques du service de téléphonie utilisé.

- Les fournisseurs de service **d'accès à l'internet** accessible au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent, « **au minimum** » les données suivantes :

  1° l'identifiant de l'utilisateur final ;
  2° l'identification et la localisation des points de terminaison du réseau utilisés par l'utilisateur final du début à la fin d'une connexion ou d'une communication ;
  3° la date et l'heure de l'ouverture et de la fermeture d'une session du service d'accès à l'internet ;
  4° le volume de données envoyées vers le réseau et téléchargées pendant la durée de la session ou autre unité de temps demandée ;
  5° les données permettant d'établir la localisation géographique des cellules en se référant à leur identifiant cellulaire au moment où la communication a été effectuée ;

- Les fournisseurs d'un **service de courrier électronique par internet accessible au public,** les fournisseurs d'un **service de téléphonie par internet accessible au public** et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

  1° l'identifiant de l'utilisateur final du compte de courrier électronique ou de téléphonie par internet, ainsi que le numéro ou l'identifiant du destinataire prévu de la communication ;
  2° le numéro de téléphone attribué à toute communication entrant dans le réseau téléphonique public dans le cadre d'un service téléphonique par internet ;
  3° a) l'adresse IP et le port source utilisés par l'utilisateur final ;

b) l'adresse IP et le port source utilisés par le destinataire ;

4° la date et l'heure de l'ouverture et de la fermeture d'une session du service de courrier électronique ou de téléphonie par internet ;

5° la date et l'heure de la connexion établie à l'aide du compte de téléphonie par Internet ;

6° les caractéristiques techniques du service utilisé.

113. L'Autorité constate que **les listes de données établies par l'arrêté du 19 septembre 2013 ne sont pas exhaustives** puisque l'arrêté royal indique que les « *fournisseurs […] conservent au minimum les données suivantes […]* »[106]. **L'exigence de prévisibilité ne peut se satisfaire d'une détermination non-exhaustive des données à conserver**. Le **projet d'arrêté sera revu** afin de veiller à ce que l'arrêté royal du 19 septembre 2013 détermine de manière exhaustive les données qui doivent être conservées par les opérateurs.

114. Par ailleurs, l'Autorité souligne que 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

115. L'Autorité n'a **pas d'autre remarque** concernant les données déterminées par l'arrêté royal du 19 septembre 2013.

- ***Commentaires portant sur le nouvel article 126/1 § 3 de la loi télécom :***

116. Le nouvel article 126/1 § 3 de la loi télécom identifie **les différentes zones géographiques dans lesquelles les opérateurs doivent conserver, de manière préventive, les données de trafic se rapportant aux communications qui y sont effectuées** (parce que l'origine ou la destination de la communication s'y trouve).

117. Il ressort de la jurisprudence européenne qu'une mesure législative peut imposer une obligation de conservation préventive « ciblée » sur base de critères géographiques afin de sauvegarder la sécurité nationale, de lutter contre la criminalité grave, de prévenir des menaces graves contre la sécurité publique et de sauvegarder des intérêts vitaux d'une personne physique. La CJUE juge, en effet, qu'une telle mesure respecte, en principe, le principe de proportionnalité. **Il convient toutefois de veiller à ce que les critères retenus par l'avant-projet de loi pour déterminer les zones géographiques dans lesquelles une obligation de conservation des données de trafic est imposée de manière préventive n'aboutissent pas à réintroduire, *de facto*, une obligation de conservation généralisée et indifférenciée des données de trafic**

[106] C'est l'Autorité qui souligne.

118. Pour rappel, la CJUE considère que les Etats ne peuvent imposer une telle obligation de conservation généralisée et indifférenciée des données de trafic que lorsque qu'il existe des circonstances suffisamment concrètes permettant de considérer que l'État membre concerné fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible. La CJUE précise que la sécurité nationale correspond à l'intérêt primordial de protéger les fonctions essentielles de l'Etat et les intérêts fondamentaux de la société et inclut la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme[107].

119. Le **nouvel article 126/1 § 3, 1° de la loi télécom** prévoit qu'une obligation de conservation des données est imposée pour les « *arrondissements judiciaires dans lesquels au moins 3 infractions visées à l'article 90ter du Code d'instruction criminelle par 1000 habitants par an ont été constatées durant l'année sur une moyenne des trois années calendriers précédentes celle en cours* » ou pour les « *zones de police, dans lesquelles, au moins 3 infractions visées à l'article 90ter du Code d'instruction criminelle par 1000 habitants par an ont été constatées sur une moyenne des trois années calendriers précédentes celle en cours, et situées dans les arrondissements judiciaires dans lesquels pendant l'année calendrier précédente celle en cours, moins de 3 infractions visées à l'article 90ter du Code d'instruction criminelle par 1000 habitants par an sur une moyenne de trois années précédente celle en cours ont été constatées* ».

120. L'article 90ter § 2 du CIC comprend une longue liste d'infractions. Il s'agit des infractions pour lesquelles « *le juge d'instruction peut, dans un but secret, intercepter, prendre connaissance, explorer et enregistrer, à l'aide de moyens techniques, des communications non accessibles au public ou des données d'un système informatique ou d'une partie de celui-ci, ou étendre la recherche dans un système informatique ou une partie de celui-ci* ». Comme l'indique le délégué du Ministre dans une réponse à des demandes d'informations complémentaires, cette liste « *wordt over het algemeen beschouwd als de lijst met de meest zware vormen van criminaliteit. De lijst wordt in het wetboek meerdere keren gebruikt als drempel voor de proportionaliteitsvereiste voor wat betreft de opsporingsmethoden die het meest ingrijpend zijn in de persoonlijke levenssfeer. Dit is o.a. het geval voor:*

- *De proactieve recherche (artikel 28bis, § 2)*
- *Het blokkeren van banktegoeden (artikel 46quater, § 2, tweede lid)*
- *De inkijkoperatie (artikel 46quinquies/89ter)*
- *De infiltratie (artikel 47octies)*
- *De observatie met gebruik van technische middelen om zicht te krijgen in de woning van een advocaat of een arts (artikel 56bis)*

[107] CJUE, arrêt du 6 octobre 2020, § 135.

- *De volledige anonimiteit van getuigen (artikel 86bis)*
- *De onderschepping en kennisname van private elektronische communicatie en de geheime zoeking in een informaticasysteem (artikel 90ter)*
- *Het toekennen van bijzondere beschermingsmaatregelen aan bedreigde getuigen (artikel 104, § 2)*
- *Het toekennen van bijzondere beschermingsmaatregelen aan bedreigde personen die een openbaar ambt uitoefenen (artikel 111quater, § 1, tweede lid)* ».

121. **L'Autorité prend note du choix du demandeur d'utiliser cette liste pour définir ce qui relève de la « criminalité grave ».**

122. Elle **s'interroge, en revanche, sur le choix du seuil de « 3 infractions 90ter par 1000 habitants par an »** pour caractériser une zone comme étant particulièrement exposée à la commission d'actes de criminalité grave. L'Exposé des motifs indique le nombre d'infractions totales qui doivent être constatées dans un arrondissement judiciaire pour qu'une obligation de conservation des données y soit imposée, mais il ne donne pas les statistiques relatives aux nombres d'infractions « 90ter » ayant effectivement été constatées dans les différents arrondissements judiciaires. L'Autorité a demandé à pouvoir obtenir ces statistiques afin d'être en mesure d'évaluer si le seuil retenu aboutit à recréer, *de facto*, une obligation généralisée et indifférenciée des données de trafic de l'ensemble des utilisateurs d'un moyen de communications électroniques. Malgré sa demande, cette information ne lui a pas été communiquée. **L'Autorité n'est dès lors pas en mesure d'apprécier la pertinence et la proportionnalité du critère retenu**. **Le législateur devra justifier le seuil qu'il retient et démontrer que celui-ci n'aboutit pas à réintroduire, *de facto*, une obligation de conservation généralisée et indifférenciée des données sur la (quasi-)totalité du territoire national**. Certes, le critère retenu (une moyenne de 3 infractions 90ter par 1000 habitants par an) est un critère dynamique et il n'est dès lors pas possible de déterminer, une fois pour toutes, s'il aboutit à recréer, *de facto*, une obligation de conservation généralisée et indifférenciée des données sur la (quasi-)totalité du territoire national. Mais **le législateur doit veiller à ce que l'impact pratique de ce seuil soit proportionné au regard des statistiques actuelles** ; ce qui ne serait pas le cas s'il aboutissait à placer, lors de l'entrée en vigueur de l'avant-projet de loi, l'entièreté (ou presque) du territoire ou de la population « sous surveillance ». **Le législateur doit réaliser une analyse rigoureuse et quantitative de la proportionnalité du critère/seuil retenu dans l'avant-projet de loi.**

123. L'avant-projet de loi prévoit que « *les statistiques utilisées proviennent de la Banque de données Nationale Générale visée à l'article 44/7 de la loi sur la fonction de police* » (ci-après « la B.N.G »). **L'Autorité en prend note, mais elle souligne que le législateur doit toutefois être en mesure d'attester que la B.N.G est la base de données la plus adéquate à cette fin**. L'Autorité

s'interroge, en effet, sur la pertinence d'utiliser la B.N.G alors que cette base de données est tenue par la police qui aura naturellement, au vu de sa mission légale, une propension à y faire figurer toutes ses suspicions d'infractions 90ter et/ou, comme l'a souligné le C.O.C. dans son avis du 21 mai 2020, à qualifier trop facilement une suspicion d'infraction comme une suspicion de délit grave au sens de l'article 90ter du C.I.C**. Dans ce contexte, l'Autorité estime qu'il serait plus adéquat d'utiliser une base de données dont la qualité des données statistiques est encadrée par la loi, à l'instar de la loi du 4 juillet 1962 relative à la statistique publique**[108].

124. Afin d'éviter que les services de police puissent être tentés de qualifier « trop facilement » une suspicion d'infraction comme un suspicion d'une infraction grave au sens de l'article 90ter du C.I.C, l'Autorité considère, en outre, que **le seuil** retenu pour déterminer si la zone est particulièrement exposée à de la « criminalité grave » **doit être calculé en tenant compte du nombre d'infractions ayant abouti à une condamnation par les tribunaux**, et non du nombre d'infractions ayant été constatées par les services de police. Le recours au nombre de condamnations offre, en effet, une plus grande garantie que la conservation des données de trafic sera « activée », comme l'exige la CJUE, « *sur la base d'éléments objectifs et non discriminatoires* »[109].

125. Le nouvel article 126/1 § 3, 3° de la loi télécom liste 16 catégories de « *zones particulièrement exposées à des menaces pour la sécurité nationale ou à des risques élevés de criminalité grave* ». Le nouvel article 126/1 § 3, 4° de la loi télécom liste 14 catégories de « *zones où il y a une menace grave potentielle pour les intérêts vitaux du pays ou pour les besoins essentiels de la population* ». Le nouvel

[108] L'article 1er bis de la loi du 4 juillet 1962 dispose que les « *statistiques sont régies par les principes suivants :*
1° Principe de licéité et de loyauté :
a) la collecte et le traitement des données se fondent soit sur une base légale ou réglementaire, soit sur le consentement du déclarant au sens de l'article 1er, § 8, de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, sous réserve des dispositions particulières prévues dans la présente loi ;
b) la collecte loyale suppose la bonne information du déclarant au sujet de la collecte et du traitement des données. Le déclarant a le droit d'obtenir des informations concernant le fondement juridique, la finalité de la collecte et les mesures de protection adoptées ;
2° Principe de finalité :
a) les données individuelles sont utilisées exclusivement à des fins statistiques, à moins que le déclarant n'ait, sans équivoque, donné son consentement à ce que les données soient utilisées à d'autres fins ;
b) les données collectées à une fin statistique déterminée ne peuvent être utilisées à d'autres fins statistiques que si ces dernières sont compatibles avec la finalité statistique originaire ;
c) les données collectées et traitées à des fins statistiques ne peuvent pas être utilisées pour compléter ou corriger les fichiers de données à finalité non-statistique, notamment administratives ;
d) aucune décision ayant pour objet ou pour effet d'affecter la situation individuelle du déclarant, ne peut être prise sur base de données individuelles recueillies à l'occasion de la réalisation d'une statistique ;
3° Principe de proportionnalité :
a) lors du choix de la méthode de collecte, la priorité est accordée à la collecte secondaire par rapport à la collecte primaire. En toute hypothèse, la collecte s'opèrera par sondage de préférence à une collecte exhaustive et les enquêtes volontaires sont à privilégier par rapport aux enquêtes obligatoires ;
b) les données sont adéquates, pertinentes et non excessives au regard de la finalité statistique déterminée, c'est-à-dire que la collecte et le traitement des données sont limités aux seules données nécessaires aux fins statistiques poursuivies ;
4° Principe d'impartialité, d'objectivité et d'indépendance professionnelle :
a) les statistiques doivent être produites et diffusées dans le respect de l'indépendance scientifique et de manière objective, professionnelle et transparente plaçant tous les utilisateurs sur un pied d'égalité ;
b) la production et la diffusion des statistiques doivent être assurées par un organisme qui dispose d'une indépendance professionnelle à l'égard aussi bien des autres services et organismes politiques, réglementaires ou administratifs que des opérateurs du secteur privé ».

[109] CJUE, arrêt du 6 octobre 2020, § 150.

article 126/1 § 3, 5° de la loi télécom liste 5 catégories de « *zones où il y a une menace potentielle grave pour les intérêts des institutions internationales accueillies sur le territoire national* ». À chaque fois, l'avant-projet de loi autorise le Roi à fixer d'autres zones par arrêté royal. L'Autorité a deux remarques à formuler à ce propos :

(i) Premièrement, l'Autorité constate que l'avant-projet de loi fait le choix de retenir de nombreux lieux pour y imposer une conservation préventive des données de trafic des communications qui y sont effectuées (soit que l'origine de la communication s'y trouve, soit que le destinataire de la communication s'y trouve). **L'Autorité souligne que le législateur doit bien veiller, au cours de la délibération précédant le vote, à apprécier la nécessité et la proportionnalité de la sélection des différents lieux retenus**[110]. Il importe, en tout état de cause, que cette sélection de lieux n'aboutisse pas à réintroduire, *de facto*, une obligation de conservation indifférenciée des données d'une proportion trop importante des utilisateurs de moyens de communications électroniques en Belgique.

(ii) Deuxièmement, et en tout état de cause, **le principe de légalité** consacré par l'article 22 de la Constitution **s'oppose à ce que le législateur puisse déléguer au Roi la possibilité d'étendre l'obligation de conservation à d'autres lieux** que ceux identifiés par l'avant-projet de loi. L'avant-projet de loi **sera modifié afin de supprimer cette possibilité**.

126. Enfin, l'Autorité estime nécessaire **qu'une transparence soit assurée** quant (1) **au pourcentage du territoire national soumis à l'obligation de conservation préventive** imposée en vertu du nouvel article 126/1 de la loi télécom et quant (2) au **pourcentage de la population concernée par cette obligation**. Une telle transparence permettrait de contrôler que les critères retenus par le législateur n'ont pas abouti à réintroduire, *de facto*, une obligation de conservation généralisée et indifférenciée des données de trafic et de localisation à des fins de lutte contre la criminalité grave alors qu'une telle obligation a été jugée disproportionnée par la CJUE. **Ces statistiques doivent être reprises dans le rapport que le Ministre des**

[110] L'Autorité se demande, par exemple, s'il est effectivement nécessaire et proportionné de prévoir une conservation des données de trafic de toutes les communications effectuées à partir de ou vers les autoroutes ou les parkings publics attenants aux autoroutes. Le délégué du Ministre indique, à la suite d'une demande d'informations complémentaires, que « *les autoroutes constituent le réseau de transport routier essentiel de notre pays. C'est grâce à celui-ci que l'approvisionnement en nourriture, énergie, etc., est assurée dans tout le pays. Il est également le réseau principal utilisé par les services qui délivrent une aide urgente à la population. Les parkings autoroutiers font partie intégrante du réseau autoroutier, ils constituent la zone de délestage de l'autoroute et sont, pour la plupart, la zone de ravitaillement en carburant des véhicules qui empruntent ces autoroutes. Vu les particularités des autoroutes (voies à grandes vitesses sans possibilité d'arrêt autre que la bande d'urgence), les parkings autoroutiers sont également des zones d'échange, de repos, etc. Le code de la route prévoit, en son article 21.4, que l'on ne peut mettre un véhicule à l'arrêt ou en stationnement que sur les aires de stationnement indiquées par le signal. La sécurité des parkings d'autoroute est importante non seulement pour les chauffeurs de camions, mais aussi pour tous les utilisateurs de ces autoroutes* ». Ces éléments ne démontrent toutefois pas la nécessité et la proportionnalité d'une obligation de conservation imposée pour les communications effectuées à partir de et vers les autoroutes.

télécommunications et le Ministre de la Justice doivent transmettre annuellement à la Chambre des représentants en vertu du nouvel article 127/2 § 1er de la loi télécom. Elles pourraient également être publiées sur le site Internet de l'IBPT, lequel doit déjà, aux termes du nouvel article 127/1 § 2 de la loi télécom, reprendre des informations générales concernant l'accès des autorités aux données conservées par les opérateurs.

127. Plus généralement, il est **essentiel que le rapport annuel transmis à la Chambre comprenne toutes les données nécessaires pour permettre une évaluation de l'efficacité et de la proportionnalité des différentes mesures de conservation** des données de trafic et de localisation. Dans cette perspective, **le rapport annuel devra, au moins, reprendre les données suivantes** :

- Les types et la quantité de données de trafic et de localisation collectées par les opérateurs en exécution des dispositions de la loi télécom et du C.I.C. (y compris le pourcentage du territoire et de la population concernée par une conservation des données en exécution du nouvel article 126/1 de la loi télécom) ;
- Le nombre de fois où une autorité a demandé à avoir accès aux données conservées par les opérateurs ;
- Les raisons pour lesquelles les autorités ont demandé (et obtenu) un accès aux données conservées par les opérateurs (sans, bien entendu, rentrer dans un exposé détaillé et concret) et des informations permettant d'établir l'utilité de cet accès.

L'avant-projet de loi sera revu afin de compléter les informations qui doivent être reprises dans le rapport annuel.

- ***Commentaires portant sur le nouvel article 126/1 § 4 de la loi télécom :***

128. Le nouvel article 126/1 § 4, alinéa 1er de la loi télécom prévoit que « *Les opérateurs conservent les données pour toutes les communications effectuées à partir d'une zone géographique visée au paragraphe 3 ou vers une telle zone* »[111]. **Afin d'assurer la clarté et la précision requise, l'avant-projet de loi précisera que « *les données* » sont les « *données visées au § 2* ».**

129. Le nouvel article 126/1 § 4, dernier alinéa 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* ». **Cette disposition est problématique au regard du principe de minimisation des données et, plus fondamentalement, du principe de la proportionnalité** qui doit régir

[111] C'est l'Autorité qui souligne.

toute mesure de conservation des données. Elle risque, en effet, d'aboutir à une conservation des données qui aille au-delà de ce qui est nécessaire et proportionné au regard des objectifs poursuivis par cette conservation. Le principe de proportionnalité, tel qu'il est interprété par la CJUE, s'oppose à ce que les opérateurs puissent conserver, en exécution de l'article 126/1 de la loi télécom, les données de trafic relatives à des communications qui sont effectuées en dehors des zones géographiques délimités par ladite disposition. Il en est d'autant plus ainsi que ces zones géographiques sont déjà déterminées de manière très large dans l'avant-projet de loi et que l'obligation de conservation des données s'impose, non seulement, aux communications « originaires » de ces zones, mais également aux communications vers ces zones. **L'avant-projet de loi sera revu afin supprimer la possibilité offerte aux opérateurs de pouvoir conserver des données au-delà des zones géographiques dans lesquelles l'avant-projet de loi impose une obligation de conservation s'ils ne leur pas techniquement pas possible de circonscrire la conservation des données à ces zones**.

130. L'Autorité insiste pour que le législateur vérifie qu'il est bien techniquement possible de mettre en place un système de conservation des données qui soit restreint à certaines zones géographiques avant d'imposer une obligation de conservation ciblée sur base de critères géographiques. **S'il n'était techniquement pas possible de circonscrire la conservation aux données de trafic relatives à des communications effectuées à certaines zones géographiques**, **le législateur ne pourra pas prévoir la mise en place d'un tel système**.

10) Détermination du responsable du traitement des traitements consistant en la conservation des données de trafic et de localisation imposées par les articles 122, 123, 126, 126/1 et 127 de la loi télécom (nouvel article 127/3 § 2 de la loi télécom)

131. Le nouvel article 127/3 § 2 de la loi télécom désigne « *chaque opérateur […] comme responsable du traitement au sens du RGPD pour les données traitées sur base des articles 122, 123, 126, 126/1 et 127* ».

132. L'Autorité **prend note de cette désignation**, **mais elle rappelle que le responsable du traitement est responsable d'un ou de plusieurs traitements, et non de données**. Ainsi, chaque opérateur est responsable du traitement des traitements visés aux articles 122, 123, 126, 126/1 et 127, et non pas des données traitées sur base de ces dispositions. **La formulation de l'article 127/3 § 2 doit être revue en ce sens.**

11) Mesures techniques et organisationnelles imposées aux opérateurs pour la conservation des données de trafic et de localisation (nouveaux articles 127/2 et 127/3 de la loi télécom)

133. Les nouveaux **articles 127/2 et 127/3** de la loi télécom entendent imposer aux opérateurs des mesures techniques et organisationnelles relatives à la conservation des données de trafic et de localisation.

134. La plupart de ces mesures sont imposées afin de garantir la sécurité des données conservées par les opérateurs. L'Autorité constate que c**es mesures visent, conformément à la jurisprudence de la CJUE, à assurer un niveau particulièrement élevé de protection et de sécurité**. Ces mesures rencontrent plusieurs exigences ayant été explicitement imposées par la CJUE, en particulier :
    - L'obligation de **conserver les données sur le territoire de l'Union européenne** (voir le nouvel article 127/2 § 3, alinéa 1, 2° de la loi télécom) ;
    - L'obligation **de détruire les données conservées de tout support lorsque le délai de conservation qui leur est applicable est expiré ou de les rendre anonymes** (voir le nouvel article 127/2 § 3, alinéa 2, 1° de la loi télécom) ;
    - L'adoption de mesures **afin de limiter le risque d'abus ou d'accès illicite aux données** (voir, notamment, le nouvel article 127 § 3, alinéa 1, 3° de la loi télécom qui impose de **rendre les données conservées pour les autorités illisibles et inutilisables**, **dès leur enregistrement, par toute personne qui n'est pas autorisée à y avoir accès** ou le nouvel article 127 § 3, alinéa 2, 4° de la loi télécom qui impose aux opérateurs **d'assurer une traçabilité de l'exploitation des données conservées à l'aide d'un journal**).

135. L'Autorité a néanmoins **plusieurs remarques** à émettre à propos de ces dispositions relatives à la sécurité des données.

136. Tout d'abord, l'Autorité constate **que l'obligation de conservation sur le territoire de l'Union européenne ne s'applique qu'aux données conservées par les opérateurs pour les autorités, et non pas aux données conservées pour leurs propres besoins** (voir le nouvel article 127/2 § 3, alinéa 1, 2° de la loi télécom). L'Autorité a **deux remarques** à ce propos :

(i) **Premièrement,** il y a un **manque de clarté sur la distinction entre données conservées pour les autorités et données conservées pour les propres besoins des opérateurs**. En effet, les nouveaux articles 122 et 123 de la loi télécom imposent des obligations de conservation à des fins de lutte contre la fraude (dont peuvent être victimes les opérateurs) et afin d'assurer la sécurité des réseaux (ce qui constitue une obligation à charge

des opérateurs). L'avant-projet prévoit, par ailleurs, que les autorités pourront, sous certaines conditions, obtenir un accès à ces données, y compris pour d'autres finalités que pour celles pour lesquelles elles ont initialement été conservées. Ces données sont-elles dès lors conservées pour les autorités ou pour les besoins propres des opérateurs ?[112]

(ii) **Deuxièmement**, l'Autorité souligne que la CJUE considère qu'en raison de la quantité de données conservées, du caractère sensible de ces données et du risque d'accès illicite à celles-ci, leur conservation sur le territoire de l'Union constitue une mesure nécessaire pour garantir un niveau particulièrement élevé de protection et de sécurité. **La CJUE ne fait pas de distinction selon la finalité pour laquelle les données sont conservées et l'Autorité n'aperçoit pas pourquoi une telle distinction serait pertinente**. **L'avant-projet sera donc modifié afin de prévoir que toutes les données conservées par les opérateurs le seront sur le territoire de l'Union**.

137. Ensuite, l'Autorité a **deux remarques principales concernant les informations qui doivent être reprises dans le journal** :

(i) L'avant-projet indique que « *le journal peut comprendre d'autres documents ou informations, pour autant que ces informations et documents ne révèlent pas d'informations confidentielles sur l'enquête menée par l'autorité, telles que sa finalité ou son contexte* ». L'Autorité souligne, au contraire, **qu'il est nécessaire que la finalité concrète pour laquelle l'accès aux données a été demandé soit ajoutée dans les informations que doit comprendre le journal** parce que cette information est nécessaire, pour permettre un contrôle effectif *a posteriori* de l'utilisation des données. Toutefois, au vu de la sensibilité de cette information, il **faut prévoir que cette information soit journalisée de manière « floutée ».**

(ii) L'avant-projet indique que « *L'opérateur adopte des mesures appropriées pour assurer la sécurité du journal et, en particulier, pour empêcher toute manipulation non autorisée de ce dernier* ». L'Autorité souligne **qu'il faut prévoir, en tout état de cause, que toute manipulation dans le journal soit, elle-même journalisée**, voire spécifier la nécessité d'introduire une impossibilité d'effacement des données reprises dans le journal.

138. Par ailleurs, l'avant-projet de loi entend imposer certaines exigences techniques et/ou organisationnelles aux opérateurs afin, semble-t-il, de garantir la disponibilité et la qualité des données conservées.

[112] L'Autorité souligne que la remarque qu'elle formule à propos du manque de clarté de la distinction entre données conservées pour les autorités et données conservées par les opérateurs pour leurs propres besoins s'applique, bien évidemment, mutatis mutandis, aux autres obligations imposées par l'article 127/3 § 3, alinéa 1er de la loi télécom.

139. Le **nouvel article 127/2 § 2, alinéa 1er,** de la loi télécom prévoit que *« Les opérateurs font en sorte que les données qu'ils conservent pour leurs propres besoins et celles qu'ils conservent pour les autorités soient accessibles de manière illimitée à partir de la Belgique* ». L'objectif et la portée de cette disposition n'apparait pas de manière évidente à sa lecture. L'Exposé des Motifs n'apporte pas d'éclairage à cet égard. À la suite d'une demande d'informations complémentaires, le délégué du Ministre a indiqué que « *Le fait que les données doivent être accessibles 'à partir de la Belgique' ne signifie pas qu'elles doivent être conservées 'en Belgique'. […] L'objectif de la phrase 'accessibles de manière illimitée à partir de la Belgique' est qu'il revient à l'opérateur de fournir les données demandées par l'autorité en Belgique. De la sorte, le droit belge reste applicable* ». Il apparait ainsi que l'objectif de cette disposition est d'imposer aux opérateurs de garantir l'accessibilité des données qu'ils conservent en tout temps, quel que soit le lieu où ces données sont conservées. **La disposition sera revue afin d'en clarifier la portée**. Cette remarque vaut, *mutatis mutandis*, pour le nouvel article 127/4, dernier alinéa, qui comprend une disposition similaire.

140. Le **nouvel article 127/2 § 2, dernier alinéa** de la loi télécom prévoit que « *Les opérateurs sont en mesure d'établir des liens entre les données conservées pour les autorités* ». Dans l'Exposé des motifs, il est indiqué qu'« *[i]l revient aux opérateurs de décider comment ils s'organisent pour la conservation des données au bénéfice des autorités (en particulier les données conservées conformément aux articles 126, 126/1, 127). Dès lors, si une même donnée est visée dans plusieurs articles, ils peuvent conserver la donnée une seule fois. Par contre, les opérateurs doivent être mesure d'établir des liens entre les données conservées pour les autorités. Ceci est nécessaire vu que pour répondre à une demande d'une autorité, un opérateur pourrait être amené à consulter des données conservées sur base de différents article*s ». À la suite d'une demande d'informations complémentaires, le délégué du Ministre a précisé que « *L'objectif est d'éviter que des données conservées soient inexploitables en l'absence de lien entre les données. Par exemple, il est essentiel que les opérateurs puissent faire un lien entre les données d'accès, de connexion, ou de communication conservées en exécution du nouvel article 126/1 avec les données d'identification conservées sur la base du nouvel article 126. Les données d'identification n'ont pas été reprises à l'article 126/1, § 2, 3°, de manière à éviter de conserver deux fois les mêmes données* ». Si l'Autorité comprend la volonté du législateur, elle souligne que la portée de l'article 127/2 § 2 ne ressort pas suffisamment de son libellé. **La disposition sera revue afin d'en clarifier la portée**. L'Autorité souligne, à ce propos, que si le législateur entend permettre aux autorités de réaliser des recherches sur des personnes concernées à partir des différentes données conservées par les opérateurs, il lui reviendrait de déterminer, dans le respect du principe de proportionnalité, les critères de recherche qui pourraient être utilisés par les autorités compétentes pour faire leurs recherches et établir les liens.

12) Conservation des données permettant l'identification des personnes concernées, de l'équipement terminal ou du service de communications électroniques employé par les fournisseurs de réseaux privés de communications électroniques et de services de communications électroniques qui ne sont pas accessibles au public (nouvel article 127/4 de la loi télécom)

141. Le **nouvel article 127/4 de la loi télécom** prévoit que le Roi doit fixer les conditions dans lesquelles les fournisseurs de **réseaux privés** de communications électroniques et de services de communications électroniques qui ne sont pas accessibles au public doivent **enregistrer et conserver les données permettant l'identification des personnes concernées, de l'équipement terminal ou du service de communications électroniques employé**. Cette obligation de conservation est imposée pour les **finalités suivante**s :

- La poursuite et la répression d'infractions pénales,
- La répression d'appels malveillants vers les services d'urgence,
- La recherche par le service de médiation pour les télécommunications de l'identité des personnes ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques,
- L'accomplissement des missions de renseignement prévues par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité

142. Le nouvel article 127/4 de la loi télécom **délègue également au Roi** le soin de **déterminer les mesures techniques et administratives imposées aux fournisseurs de réseaux privés** de communications électroniques et de services de communications électroniques qui ne sont pas accessibles au public **en vue de permettre l'identification des personnes concernées, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des communications privées** aux conditions prévues par les articles 46bis, 88bis, et 90ter à 90decies, et 464/13, 464/25 et 464/26 du Code d'instruction criminelle, ainsi qu'aux conditions prévues par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

143. L'Autorité rappelle que le principe de légalité exige que les éléments essentiels d'un traitement de données, qui constitue une ingérence importante dans les droits fondamentaux des personnes concernées, soient déterminés par une norme législative formelle. Il convient, en outre, que cette norme soit suffisamment claire et précise pour que les personnes concernées puissent appréhender de manière prévisible les circonstances dans lesquelles le traitement de données est autorisé. Il s'ensuit que **les notions fondamentales utilisées pour circonscrire la portée de l'obligation de conservation de données doivent être définies par la législation**. Or, sauf erreur, **les notions de « fournisseurs de réseaux privés de communications électroniques » et de « fournisseurs de services de communications électroniques qui ne sont pas**

accessibles au public » ne sont pas définies par la loi télécom. Comme l'Autorité vient de le souligner, **il s'agit pourtant d'un élément essentiel** des traitements de données imposés par l'article 127/4 de la loi télécom **puisque la définition de ces notions impactera la portée des obligations** de conservation qu'il impose. En effet, la notion de « réseaux privés » a-t-elle vocation à viser uniquement les réseaux des entreprises ou n'importe quel réseau privé, y compris, ceux qui sont mis en place par une personne à son domicile ? Par ailleurs, la notion a-t-elle vocation à viser les réseaux crées par n'importe quelle entreprise ou le législateur entend-t-il imposer des obligations de conservation uniquement si l'entreprise a atteint une certaine taille ? **L'avant-projet sera revu afin d'apporter une définition à ces notions, étant entendu que la définition de ces notions** – et les obligations de conservation qui devront être mises en place en fonction de ces définitions – **devra respecter les principes de nécessité et de proportionnalité**.

144. L'Autorité souligne que l'avant-projet peut, en revanche, déléguer au Roi – comme il le fait – la détermination des modalités techniques relatives aux obligations de conservations imposées par le nouvel article 127/4 de la loi télécom.

13)Accès aux données

145. Le nouvel article 127/1 de la loi télécom identifie les catégories d'autorités qui peuvent avoir accès aux données conservées par les opérateurs en exécution des articles (nouveaux) 122, 123, 126, 126/1 et 127 de la loi télécom.

146. Il ressort d'une lecture de l'article 127/1 de la loi télécom à la lumière des articles 122, 123, 126, 126/1 et 127 de la loi télécom que les **autorités qui poursuivent l'une des finalités** visées à l'article 127/1 de la loi télécom **peuvent avoir accès aux données conservées en vertu des** (nouvelles versions des) **articles 122, 123, 126 et 127 pour chacune des finalités énoncées par cet article 127/1** de la loi télécom.

147. Les nouveaux articles 126 et 127 de la loi télécom prévoient que les données qui doivent être conservées sur pied de ces dispositions sont « *conservées pour les autorités et les finalités visées à l'article 127/1* ».

148. Les articles 122 et 123 de la loi télécom autorisent ou imposent, en revanche, des obligations de conservation pour des finalités spécifiques (la facturation, le marketing des services à valeur ajouté, la lutte contre la fraude et utilisation malveillante du réseau ou encore la sécurité des réseaux et le bon fonctionnement des services de communication). Mais le nouvel article 127/1 prévoit que les autorités compétentes pour poursuivre l'une des finalités qui y est énoncée **peuvent avoir accès à toutes les données qui sont conservées en application de ces articles 122 et 123 de la loi télécom**,

même si leur conservation a initialement été autorisée ou imposée pour une autre finalité que celle qui est poursuivie par l'autorité qui veut obtenir l'accès auxdites données[113].

149. Enfin, concernant les **données conservées en vertu du nouvel article 126/1,** une lecture combinée des articles 126/1 et 127/1 de la loi télécom indique que les **autorités qui poursuivent l'une des finalités** visées à l'article 127/1 de la loi télécom **peuvent avoir accès à ces données uniquement pour les finalités pour lesquelles elles sont conservées**, à savoir aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique et de la sauvegarde des intérêts vitaux d'une personne physique.

150. Par ailleurs, l'article 127/1 de la loi télécom précise que les **autorités ne peuvent avoir accès aux données conservés par les opérateurs que dans le respect des conditions prévues par les dispositions qui les y habilitent**.

151. L'Autorité a **plusieurs remarques** à formuler à propos des dispositions encadrant la possibilité pour les autorités d'avoir accès aux données conservées par les opérateurs.

152. Tout d'abord, l'Autorité rappelle que la CJUE a jugé que **l'accès à des données de trafic et de localisation conservées par les opérateurs ne peut, en principe, être justifié que par l'objectif d'intérêt général pour lequel cette conservation a été imposée**. Il s'ensuit, en particulier, *« qu'un accès à de telles données à des fins de poursuite et de sanction d'une infraction pénale ordinaire ne saurait en aucun cas être accordé lorsque leur conservation a été justifiée par l'objectif de lutte contre la criminalité grave ou, a fortiori, de sauvegarde de la sécurité nationale.* ***En revanche, conformément au principe de proportionnalité*** *[…],* ***un accès à des données conservées en vue de la lutte contre la criminalité grave*** *peut, pour autant que soient respectées les conditions matérielles et procédurales entourant un tel accès […],* ***être justifié par l'objectif de sauvegarde de la sécurité nationale*** »[114]. En outre, la CJUE estime qu'il *« est loisible aux États membres de prévoir dans leur législation qu'un accès à des données relatives au trafic et à des données de localisation peut, dans le respect de ces mêmes conditions matérielles et procédurales, avoir lieu à des fins de lutte contre la criminalité grave ou de sauvegarde de la sécurité nationale lorsque lesdites données sont conservées par un fournisseur d'une manière conforme aux articles 5, 6 et 9 ou encore à l'article 15, paragraphe 1, de la directive 2002/58* »[115]. **Le législateur peut donc prévoir que les autorités peuvent accéder aux données conservées en application des**

[113] En effet, les nouveaux articles 122 § 7 et 123 § 6 de la loi télécom prévoient, chacun, que « *cet article [à savoir, respectivement, l'article 122 et l'article 123] ne porte pas préjudice à l'article 127/1* ». Le nouvel article 126 § 1, alinéa 3, prévoit que « Ces données sont conservées pour les autorités et les finalités visées à l'article 127/1 » et le nouvel article 127 § 1, alinéa 2, prévoit que « *Ces données et documents sont conservés pour les autorités et les finalités visées à l'article 127/1* ».
[114] CJUE, arrêt du 6 octobre 2020, § 166 (c'est l'Autorité qui met en gras).
[115] CJUE, arrêt du 6 octobre 2020, § 166 (c'est l'Autorité qui met en gras).

articles 122 et 123 pour d'autres finalités que celles qui étaient poursuivies par leur conservation initiale, mais uniquement si ces finalités de traitement ultérieur relèvent de la sauvegarde de la sécurité nationale ou de la lutte contre la criminalité grave (ou d'un autre objectif listé à l'article 15 de la Directive ePrivacy qui présente un degré d'importance similaire). Dans sa version actuelle, l'avant-projet de loi permet une réutilisation des données conservées en application des articles 122 et 123 pour toutes les finalités reprises à l'article 127/1 de la loi télécom et pas seulement les finalités présentant une certaine gravité/importance, à l'instar de la lutte contre la criminalité grave. Cette possibilité n'est pas conforme aux exigences européennes. **L'avant-projet sera dès lors revu afin d'y inscrire cette limitation concernant les finalités pour lesquelles une utilisation ultérieure des données conservées en application des articles 122 et 123 est possible**.

153. Par ailleurs, **l'Autorité rappelle que l'accès aux données doit être subordonné au respect des conditions matérielles et procédurales identifiées par la CJUE**. L'avant-projet de loi précise, à cet égard, que les autorités ne peuvent avoir accès aux données que « *dans les conditions prévues par les dispositions qui les y habilitent* ». Ce sont donc ces dispositions qui doivent prévoir les conditions matérielles et procédurales nécessaires. **Pour rappel, ces conditions sont les suivantes** :

- La réglementation nationale concernée **doit se fonder sur des critères objectifs pour définir les circonstances et les conditions dans lesquelles l'accès aux données doit être accordé.**
- L'accès des autorités nationales compétentes aux données conservées doit, en principe, sauf cas d'urgence dûment justifiés, être subordonné **à un contrôle préalable** effectué soit par une juridiction soit par une entité administrative indépendante. La décision de cette juridiction ou de cette entité doit intervenir à la suite d'une demande motivée de ces autorités.
- Les autorités qui ont eu accès aux données doivent **en informer les personnes concernées** dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes menées par ces autorités.

154. **Il incombe au législateur de vérifier que toutes les dispositions qui habilitent les autorités à avoir accès aux données de trafic et de localisation conservées par les opérateurs prévoient les conditions matérielles et procédurales nécessaires afin de respecter les exigences européennes**. Les dispositions qui organisent l'accès des autorités aux données conservées par les opérateurs se retrouvent dans les lois organiques de ces autorités, lesquelles sont, pour la plupart, préexistantes à l'avant-projet de loi. Celui-ci apporte toutefois quelques modifications à des dispositions qui organisent l'accès de certaines autorités aux données conservées par les opérateurs. L'Autorité examine si ces modifications respectent les exigences issues de la jurisprudence

européenne (mais son examen se limite aux modifications apportées). C'est ainsi que l'Autorité a constaté que **l'avant-projet de loi prévoit de permettre à certaines autorités d'avoir accès aux données conservées par les opérateurs sans exiger que cet accès fasse l'objet d'une autorisation préalable par une juridiction ou par une entité administrative indépendante qui ait la qualité de tiers** par rapport à l'autorité qui cherche à avoir accès aux données. C'est le cas, notamment, pour les autorités suivantes :

- L'avant-projet prévoit que l'IBPT « *peut demander aux opérateurs les données d'identification, de trafic ou de localisation, au sens de la loi du 13 juin 2005 relative aux communications électroniques, pour autant que cela soit nécessaire à l'accomplissement de l'une de ses missions* » (article 17 de l'avant-projet de loi)
- L'avant-projet de loi prévoit que le CCB peut, « *[l]orsque cela s'avère strictement nécessaire à la réalisation de ses tâches énumérées à l'article 60, a) à e), de la présente loi, […] obtenir des opérateurs, au sens de l'article 2, 11°, de la loi du 13 juin 2005 relative aux communications électroniques, des données d'identification, de trafic ou de localisation conservées par ceux-ci* » (article 34 de l'avant-projet de loi)
- L'avant-projet de loi prévoit que les membres du personnel statutaire ou contractuel du SPF Santé publique, Sécurité de la chaîne alimentaire et Environnement « *peuvent identifier les personnes physiques et morales sur la base de leur numéro de téléphone ou de l'adresse IP à la source de la communication électronique. À cette fin, ils peuvent, sur requête dûment motivée, demander la mise à disposition de documents et de données d'identification* » aux opérateurs (article 33 de l'avant-projet de loi).
- L'avant-projet de loi prévoit qu' *« un officier de police judiciaire de la Cellule des Personnes Disparues de la police fédérale peut, dans le cadre de sa mission d'assistance à personne en danger et de recherche de personnes dont la disparition est inquiétante, et lorsqu'il existe des présomptions ou indices sérieux que l'intégrité physique de la personne disparue se trouve en danger imminent, requérir d'obtenir les données relatives aux communications électroniques concernant la personne disparue* » (article 19 de l'avant-projet).

155. L'absence (systématique) de contrôle préalable à la communication des données n'est pas admissible[116]. **L'avant-projet sera revu afin de veiller à ce que l'accès aux données soit,**

[116] À la suite d'une demande d'informations complémentaires, le délégué du Ministre indique que la CJUE n'imposerait pas une exigence de contrôle préalable à l'accès des données lorsque cet accès a lieu dans un autre contexte que la recherche, la prévention, la détection ou la poursuite d'infractions pénales. L'Autorité ne peut souscrire à cette interprétation. Certes, la CJUE a identifié les différentes conditions matérielles et procédurales qui doivent subordonner l'accès des autorités aux données conservées par les opérateurs dans le cadre de décisions examinant la conformité de législations nationales organisant l'accès des autorités aux données de trafic dans le cadre de procédures de prévention, de détection ou de poursuites pénales. Cependant, la Cour n'a pas limité ces exigences à ce seul contexte. En effet, la CJUE a jugé, dans un arrêt du 21 décembre 2016, qu' « *il est essentiel que l'accès des autorités nationales compétentes aux données conservées soit, en principe, sauf cas d'urgence dûment justifiés, subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante, et que la décision de cette juridiction ou de cette entité intervienne à la suite d'une demande motivée de ces autorités présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénales* » (C'est l'Autorité qui souligne). Dans un arrêt du 2 mars 2021, la CJUE a jugé que « *Ce contrôle préalable requiert entre autres, […],*

conformément aux exigences européennes, toujours subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante qui présente la qualité de tiers par rapport à l'autorité demandant l'accès aux données, **sauf dans les cas d'urgence dûment justifiés**[117]**.**

que la juridiction ou l'entité chargée d'effectuer ledit contrôle préalable dispose de toutes les attributions et présente toutes les garanties nécessaires en vue d'assurer une conciliation des différents intérêts et droits en cause. S'agissant plus particulièrement d'une enquête pénale, un tel contrôle exige que cette juridiction ou cette entité soit en mesure d'assurer un juste équilibre entre, d'une part, les intérêts liés aux besoins de l'enquête dans le cadre de la lutte contre la criminalité et, d'autre part, les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel des personnes dont les données sont concernées par l'accès » (C'est l'Autorité qui souligne**). Les éléments soulignés laissent clairement sous-entendre que le contrôle préalable à l'accès aux données a, selon la CJUE, également un rôle à jouer en dehors des situations où l'accès aux données est demandé en vue de prévenir, détecter ou poursuivre des infractions pénales**. **L'objectif poursuivi par l'exigence de contrôle préalable par une juridiction ou une autorité administrative indépendante est de s'assurer que les autorités n'ont accès qu'aux données de trafic auxquelles elles peuvent effectivement avoir accès ; ces données devant être limitées à ce qui est strictement nécessaire aux fins d'atteindre l'objectif poursuivi par la demande d'accès.** Ce contrôle préalable est particulièrement important parce que l'accès aux données de trafic constitue une ingérence qui peut être particulièrement grave dans les droits au respect de la vie privée et à la protection des données à caractère personnel puisque ces données sont susceptibles de fournir des informations précises sur la vie privée d'un utilisateur d'un moyen de communications électroniques, même lorsque l'accès ne porte que sur une quantité limitée de données ou sur des données limitées à une courte période (voyez, les arrêts suivants de la CJUE : arrêt du 8 avril 2014, § 62 ; arrêt du 21 décembre 2021, § 118-120 ; arrêt du 2 mars 2021, § 40). **Les éléments qui justifient la nécessité d'un contrôle préalable existent tant lorsque l'accès des autorités a lieu dans le cadre d'une procédure pénale que lorsque cet accès intervient dans un autre contexte**. L'existence de voies de recours juridictionnels (*a posteriori*) ne peut suffire à rencontrer l'exigence d'un contrôle préalable.

[117] Le délégué du Ministre a justifié l'absence de contrôle préalable à l'accès aux données par un officier de police judiciaire de la Cellule des Personnes Disparues de la police fédérale dans le cadre d'une recherche concernant des personnes disparues à l'aide de deux éléments : 1) le fait que la Cellule des Personnes Disparues n'œuvre pas dans le cadre d'une finalité « pénale » et 2) le fait qu'un recours à une procédure d'autorisation préalable pourrait avoir pour conséquence de faire perdre aux services de recherche des heures, voire des jours, qui s'avèrent souvent cruciaux dans le succès de la recherche de la personne concernée et dans la protection de ses intérêts vitaux. L'Autorité ne peut suivre le demandeur dans son premier argument. Cependant, l'existence d'une urgence particulière, qui est dûment justifiée, peut justifier de se passer de contrôle préalable. La législation pourrait dès lors prévoir une exception à l'obligation de contrôle préalable de la demande d'accès aux données d'un officier de police judiciaire de la Cellule des Personnes Disparues en cas d'urgence, étant entendue que celle-ci devrait être dûment justifiée (et évaluée au cas par cas). Le délégué du Ministre avance un argument similaire pour justifier l'absence de contrôle préalable à l'accès aux données de trafic par le CCB : « *En raison de l'augmentation, de la fréquence des incidents en matière de cybersécurité et de la rapidité de réaction nécessaire, le CCB ne pourrait prévenir et détecter en temps utile les infractions en matière de cybercriminalité, les menaces contre la sécurité publique liées à la cybersécurité et les défaillances de la sécurité des réseaux s'il devait obtenir systématiquement l'autorisation préalable d'une juridiction ou d'une autorité nationale indépendante pour accéder à ces données de communications électroniques* ». A nouveau, l'Autorité souligne que l'existence d'une urgence particulière, qui est dûment justifiée, peut justifier de se passer de contrôle préalable, mais cette appréciation doit se faire *in concreto* et ne peut être décrétée par principe.

Le délégué du Ministre a justifié l'absence de contrôle préalable à l'accès aux données par les membres du personnel statutaire ou contractuel du SPF Santé publique parce que les données sur lesquelles peuvent porter une demande d'accès sont limitées aux données strictement nécessaires afin de pouvoir identifier un utilisateur et que ces données sont considérées comme « moins sensibles ». À nouveau, l'Autorité ne peut souscrire à cette motivation. D'ailleurs, dans l'arrêt invoqué par le demandeur à l'appui de son raisonnement (arrêt du 2 octobre 2018, *Ministerio fiscal*), l'accès aux données d'identification était soumis à un contrôle judiciaire préalable. Ce contrôle est nécessaire pour s'assurer que l'accès de l'administration aux données d'identification répond bien aux exigences légales (y compris de nécessité et de proportionnalité). Par ailleurs, le délégué du Ministre indique que « *il est utile de préciser que ce pouvoir est prévu par l'article 14, c, du Règlement 2019/1020 du Parlement européen et du Conseil du 20 juin 2019 sur la surveillance du marché et la conformité des produits, et modifiant la directive 2004/42/CE et les règlements (CE) no 765/2008 et (UE) no 305/2011* ». L'Autorité souligne, à cet égard, que ledit Règlement européen dispose que « *les autorités de surveillance du marché exercent les pouvoirs énoncés au présent article de manière effective et efficace, conformément au principe de proportionnalité, dans la mesure où cet exercice se rapporte à l'objet et à l'objectif des mesures, à la nature de la non-conformité et au dommage global, potentiel ou avéré, découlant d'un cas de non-conformités. Ces pouvoirs sont conférés et exercés conformément au droit de l'Union et au droit national, y compris aux principes de la Charte des droits fondamentaux de l'Union européenne, et aux principes du droit national relatifs à la liberté d'expression ainsi qu'à la liberté et au pluralisme des médias, aux garanties procédurales applicables et aux règles de l'Union concernant la protection des données, en particulier le règlement (UE) 2016/679* » (c'est l'Autorité qui souligne). Soumettre l'exercice du pouvoir de « *demander aux opérateurs économiques de fournir des informations pertinentes aux fins de l'identification du propriétaire d'un site internet, dès lors que cette information a trait à l'objet de l'enquête* » à un contrôle préalable est autorisé par le Règlement 2019/1020 parce que cela s'impose en vertu du droit au respect des données à caractère personnel tel qu'il a été interprété par la CJUE dans ses arrêts relatifs à la conservation des données de trafic.

156. L'Autorité rappelle également que la juridiction ou l'autorité administrative indépendante qui procède au contrôle préalable doit s'assurer que la communication de données poursuit une des finalités pour laquelle cette communication peut avoir lieu. À cet égard, l'Autorité rappelle que la communication de données ne peut, en principe, être justifiée que par l'objectif d'intérêt général pour lequel la conservation a été imposée, à moins que la loi permette, dans le respect du principe de proportionnalité, une communication pour d'autres finalités. Il convient, en outre, que la juridiction ou l'autorité administrative indépendante veille à la proportionnalité de la communication de données avant de l'autoriser.

157. Par ailleurs, concernant la possibilité pour l'IBPT d'avoir accès aux données de trafic nécessaires à l'exercice de ses missions, l'Exposé des Motifs indique que cet accès est nécessaire, par exemple, pour permettre à l'IBPT de contrôler le « *respect par les opérateurs de leurs obligations légales, telles que l'obligation d'adresser une facturation détaillée, prévue à l'article 110 de la loi du 13 juin 2005 relative aux communications électroniques, ou dans le cadre de la mise en œuvre de l'article 114 de cette même loi. Par exemple, en matière de facturation détaillée, l'IBPT doit être en mesure de demander à l'opérateur de lui fournir un échantillon de factures. Or, ces factures reprennent des données de trafic, telles que les destinataires, dates, heures et durées des communications passées* ». Afin d'assurer la prévisibilité de la loi et de veiller à la nécessité ainsi qu'à la proportionnalité de l'ingérence qui résulte de l'accès à des données de trafic, **l'avant-projet de loi doit identifier explicitement les missions pour lesquelles l'IBPT peut avoir accès aux données de trafic conservées par les opérateurs**.

14) Règles particulières insérées par l'avant-projet de loi concernant l'usage de la cryptographie dans le domaine des communications électroniques

158. Le nouvel article 127/5 § 1 de la loi télécom interdit « *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 ou la fourniture des données d'identification de l'appelant ;
2° l'identification de l'utilisateur final, le repérage et la localisation des communications non accessibles au public 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 ;
3° les écoutes, la prise de connaissance et l'enregistrement des communications non accessibles au public 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 ».

159. Cette interdiction est déjà (partiellement) inscrite dans la version actuelle de la loi télécom (voir l'article 127 actuel de la loi télécom).

160. Le nouvel article 127/5 § 2 de la loi télécom apporte **des dérogations au principe selon lequel *« l'emploi de la cryptographie est libre »***[118] :

- Il est interdit de fournir ou d'utiliser un système d'encryptage qui empêche les communications d'urgence (nouvel article 127/5 § 2, alinéa 2 de la loi télécom).
- Les systèmes d'encryptage, qui peuvent être utilisés pour garantir la confidentialité des communications et la sécurité des paiements, ne peuvent pas empêcher la conservation par l'opérateur des données d'identification, de trafic ou de localisation pour les autorités (nouvel article 127/5 § 2, alinéa 3 de la loi télécom).Lorsqu'un opérateur met en place un système d'encryptage qui peut être utilisé pour garantir la confidentialité des communications et la sécurité des paiements, il doit rendre possible, dans les 24h à partir de la transmission de la requête, les mesures d'interception légale, en particulier l'identification de l'utilisateur final, le repérage et la localisation des communications non accessibles au public ainsi que les écoutes, la prise de connaissance et l'enregistrement des communications non accessibles au public. L'opérateur rend possible la réalisation de ces opérations uniquement pour les communications visées dans la requête et qui sont postérieures à celles-ci (nouvel article 127/5 § 2, alinéas 4 et 5 de la loi télécom).

161. L'Autorité a **deux remarques fondamentales** à formuler à propos des interdictions imposées par cette disposition.

162. Premièrement, 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 **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. **L'avant-projet de loi sera revu afin de supprimer cette interdiction**.

163. Deuxièmement, l'Autorité souligne qu'en imposant aux opérateurs qui mettent en place un système d'encryptage de rendre les mesures d'interception légale possibles, en particulier l'identification de l'utilisateur final, le repérage et la localisation des communications ainsi que les écoutes, la prise de connaissance et l'enregistrement des communications non accessibles au public, le nouvel article 127/5 § 2 de la loi télécom impose *de facto* l'insertion de « portes dérobées » (« *backdoors* ») dans les systèmes de cryptographie afin de pouvoir déchiffrer les messages encryptés. Or l'Autorité relève qu'il existe, depuis les années 1990, un consensus fort

[118] Ce principe est actuellement consacré par l'article 48 de la loi télécom. Lorsque la loi transposant le CCEE aura été adoptée, ce principe sera consacré par le nouvel article 105/4 de la loi télécom (qui reproduit l'article 48 actuel de la loi télécom).

dans la communauté scientifique pour considérer que l'insertion de « portes dérobées » (« *backdoors* ») dans les systèmes de cryptographie présente plus de risques pour la vie privée des personnes concernées et les intérêts supérieurs des Etats que d'avantages en termes de lutte contre la criminalité grave[119]. **L'avant-projet de loi doit dès lors être revu afin de supprimer l'obligation pour les opérateurs qui mettent en place un système d'encryptage de rendre possible les mesures d'interception légale**. Certes, les systèmes de cryptographies ont rendu l'accès au contenu des communications plus difficile qu'auparavant. Mais l'Autorité souligne qu'il existe néanmoins déjà beaucoup d'informations « digitales » disponibles sur les équipements terminaux des utilisateurs (log, cookies, mémoire flash qui ne peut être effacée…), auprès des opérateurs (données collectées en vue de la facturation, par exemple) ainsi que dans l'espace public (caméras de surveillance, caméras ANPR,…). L'Autorité souligne, encore, que si cela s'avère nécessaire en vue de lutter contre la criminalité grave, les autorités peuvent « hacker » les appareils téléphoniques pendant leur utilisation (Encrochat, SKY ECC, Hacking team, NSO group...) ou encore faire appel à des techniques particulières de recherche (comme l'infiltration, l'observation à l'aide de moyens techniques, le recours aux indicateurs, …). L'Autorité constate que ces différents moyens, qui sont mis à la disposition des autorités répressives, rendent, sans doute, la lutte contre la criminalité grave plus facile qu'auparavant et qu'en tout cas, il n'existe aucune preuve du contraire. Dans ces conditions – et au regard des risques, notamment, de « mise sur écoute » de citoyen.ne.s, y compris d'hommes et de femmes politiques (comme l'a été Angela Merkel pendant 5 ans) ou encore de chef.fe.s d'entreprises, notamment, par des pays tiers – **l'Autorité insiste pour que le demandeur supprime les dérogations au principe selon lequel « l'emploi de la cryptographie est libre ».**

15) Remarque finale

164. L'article 1er de l'arrêté du 19 septembre 2013 dispose que « *Le présent arrêté transpose partiellement la Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la Directive 2002/58/CE (directive « conservation de données ») (J.O. C.E. 13 avril 2006, L 105/54) et l'article 15.1 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*

[119] Voyez, par exemple, The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption, https://academiccommons.columbia.edu/doi/10.7916/D8GM8F2W (1997), Keys under doormats, https://www.lawfareblog.com/keys-under-doormats-mandating-insecurity (2015); US National Academies, Decrypting the Encryption Debate, https://www.nap.edu/read/25010/chapter/1 (2018); https://static.newamerica.org/attachments/3138--113/Encryption_Letter_to_Obama_final_051915.pdf; https://www.vice.com/en/article/8qxwda/former-nsa-chief-strongly-disagrees-with-current-nsa-chief-on-encryption; https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate; https://blog.cryptographyengineering.com/2018/04/26/a-few-thoughts-on-ray-ozzies-clear-proposal/; https://carnegieendowment.org/2019/09/10/moving-encryption-policy-conversation-forward-pub-79573

communications électroniques (directive « vie privée et communications électroniques ») (J.O.C.E. 31 juillet 2002, L 201/37) ». Ainsi, l'Autorité constate que cette disposition fait encore référence à la directive 2006/24 alors que celle-ci a été invalidée par la CJUE en 2014. **L'arrêté du 19 septembre 2013 sera modifié pour supprimer cette référence à une directive invalide.**

PAR CES MOTIFS,

L'Autorité estime que les adaptations suivantes doivent être apportées à l'avant-projet de loi et au projet d'arrêté :

- Réaliser une analyse rigoureuse de la nécessité et de la proportionnalité de l'obligation de conserver les données de localisation et autres données de trafic nécessaires afin de détecter et d'analyser une fraude présumée ou une utilisation malveillante présumée du réseau de communication électroniques et adapter le projet en conséquence et/ou mentionner les justifications pertinentes dans l'exposé des motifs (cons. 67-69)

- Si, après analyse, le législateur estime qu'il est rigoureusement nécessaire et proportionné d'imposer une obligation de conservation des données de trafic à des fins de lutte contre la fraude et l'utilisation malveillante du réseau, les adaptations suivantes doivent être apportées :
  - Déterminer les données précises qui doivent être conservées en application de cette obligation ou imposer au Roi d'intervenir pour déterminer ces données (cons. 72)
  - Préciser que la possibilité de conserver les données au-delà du délai minimal de 4 mois concerne les situations où une conservation plus longue est nécessaire pour gérer un contentieux relatif à une fraude ou à une utilisation malveillante du réseau (cons. 73)

- Réaliser une analyse rigoureuse de la nécessité et de la proportionnalité de l'obligation de conserver les données de localisation et autres données de trafic nécessaires afin d'assurer la sécurité et le bon fonctionnement des réseaux et des services de communications électroniques et adapter le projet en conséquence et/ou mentionner les justifications pertinentes dans l'exposé des motifs (cons. 78-80)

- Si, après analyse, le législateur estime qu'il est rigoureusement nécessaire et proportionné d'imposer une obligation de conservation des données de trafic afin

d'assurer la sécurité et le bon fonctionnement des réseaux et des services de communications électroniques, les adaptations suivantes doivent être apportées :

- Déterminer les données précises qui doivent être conservées en application de cette obligation ou imposer au Roi d'intervenir pour déterminer ces données (cons. 82)
- Apprécier, et, le cas échéant, justifier à l'aide d'éléments concrets, la raison pour laquelle les données doivent être conservées pendant une durée de 12 mois (cons. 83)
- Préciser que la possibilité de conserver les données au-delà du délai de 12 mois concerne les situations où une conservation plus longue est nécessaire pour gérer un contentieux relatif à une attaque ou des actes portant atteinte à la sécurité du réseau ou au bon fonctionnement du service à une fraude ou à une utilisation malveillante du réseau (cons. 83)

- Préciser que l'obligation légale prévue par les articles 122 § 4/2 et 123 ne peut être imposée que par une norme législative formelle (cons. 85 et 89)

- Réaliser une analyse rigoureuse de la nécessité et de la proportionnalité de l'obligation de conserver les données de localisation autres que des données de trafic pour les différentes finalités identifiées par le nouvel article 123 de la loi télécom et adapter le projet en conséquence et/ou mentionner les justifications pertinentes dans l'exposé des motifs (cons. 87-88)

- Le cas échéant, déterminer, au moins, les conditions dans lesquelles les opérateurs pourront conserver et traiter les données de localisation autres que des données de trafic et les durées maximales de conservation de ces données (cons. 88)

- Prévoir que les adresses IP attribuées à la source d'une connexion ne pourront être conservées qu'afin de permettre la poursuite d'objectifs particulièrement importants à déterminer (cons. 97, 100)

- Préciser que seules les adresses IP attribuées à la source d'une connexion, à l'exclusion des adresses IP attribuées à la destination d'une communication, peuvent être conservées en exécution du nouvel article 126 de la loi télécom (cons. 101)

- Prévoir que la conservation préventive et systématique des numéros d'identification des terminaux des utilisateurs finaux est imposée uniquement afin de poursuivre des objectifs présentant une importance particulière qui doivent être déterminés (comme

la lutte contre la criminalité grave), que la durée de leur conservation est strictement limitée au regard de cet objectif et prévoir des conditions et des garanties strictes quant à l'exploitation de ces données (cons. 102)

- Supprimer la possibilité offerte aux opérateurs d'avoir recours à la technique de reconnaissance faciale (ou à toute autre technique reposant sur une utilisation des données biométriques) pour identifier leurs abonnés (cons. 104)

- Déterminer les données et documents d'identification à collecter et à conserver par l'opérateur ou imposer au Roi de procéder à cette détermination (cons. 105)

- Définir la notion de « données de communication » (cons. 109)

- Définir la notion de « données des appels infructueux » ou remplacer cette expression par celle de « données de trafic des appels infructueux » (cons. 110)

- Supprimer les mots « au minimum » dans l'arrêté du 19 septembre afin de veiller à ce que cet arrêté détermine de manière exhaustive les données à conserver en exécution du nouvel article 126/1 de la loi télécom (cons. 113)

- S'assurer que le seuil retenu pour déterminer si une zone est particulièrement exposée à la commission d'actes de criminalité grave n'aboutit pas à réintroduire, de facto, une obligation de conservation généralisée et indifférenciée des données sur la (quasi-) totalité du territoire national (cons. 117)

- Veiller à ces que les modalités utilisées pour déterminer si une zone est particulièrement exposée à la commission d'actes de criminalité grave sont adéquates (cons. 122-124)

- Veiller à ce que la sélection des lieux retenus pour y cibler une conservation préventive des données réponde aux exigences de nécessité et de proportionnalité (cons. 125)

- Supprimer la délégation au Roi l'autorisant à ajouter d'autres lieux à ceux listés par l'avant-projet de loi (cons. 125)

- Compléter les informations qui doivent être reprises dans le rapport annuel que le Ministre des Télécommunications et le Ministre de la Justice doivent transmettre annuellement à la Chambre (cons. 126-127).

- Préciser que les « données » sont les « données visées au § 2 » (cons. 128)

- Supprimer la possibilité offerte aux opérateurs de pouvoir conserver des données au-delà des zones géographiques dans lesquelles l'avant-projet de loi impose une obligation de conservation s'ils ne leur pas techniquement pas possible de circonscrire la conservation des données à ces zones (cons. 129-130)

- Revoir la formulation de la désignation du responsable du traitement (cons. 132)

- Prévoir que toutes les données conservées par les opérateurs le seront sur le territoire de l'Union (cons. 136)

- Prévoir que les informations suivantes doivent être reprises dans le journal :
  - ✓ La finalité concrète pour laquelle l'accès aux données a été demandé, étant entendu que cette finalité doit être « floutée » (cons. 137)
  - ✓ Toute manipulation dans le journal (cons. 137)

- Clarifier la portée du nouvel article 127/2 § 2, alinéa 1er **et** dernier alinéa (cons. 139-140)

- Définir les notions de « fournisseurs de réseaux privés de communications électroniques » et de « fournisseurs de services de communications électroniques qui ne sont pas accessibles au public » (cons. 143)

- Prévoir que les autorités peuvent accéder aux données conservées en application des articles 122 et 123 pour d'autres finalités que celles qui étaient poursuivies par leur conservation initiale uniquement si ces finalités de traitement ultérieur relèvent de la sauvegarde de la sécurité nationale ou de la lutte contre la criminalité grave (ou d'un autre objectif listé à l'article 15 de la Directive ePrivacy qui présente un degré d'importance similaire) (cons. 152)

- Revoir les dispositions pertinentes pour s'assurer que l'accès aux données soit, conformément aux exigences européennes, toujours subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante qui présente la qualité de tiers par rapport à l'autorité demandant l'accès aux données, sauf dans les cas d'urgence dûment justifiés (cons. 153-155)

- Identifier explicitement les missions pour lesquelles l'IBPT peut avoir accès aux données de trafic conservées par les opérateurs (cons. 157).

- Supprimer 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 (cons. 162)

- Supprimer l'obligation faite aux opérateurs qui mettent en place un système d'encryptage de rendre possible les mesures d'interception légale (cons. 163).

- Supprimer, dans l'arrêté du 19 septembre 2013, la référence à la Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la Directive 2002/58/CE qui a été invalidée par la CJUE (cons. 164).

L'Autorité attire l'attention sur les éléments suivantes :

- Le législateur doit vérifier que toutes les dispositions qui habilitent les autorités à avoir accès aux données de trafic et de localisation conservées par les opérateurs prévoient les conditions matérielles et procédurales nécessaires afin de respecter les exigences européennes (cons. 154)

- La juridiction ou l'autorité administrative indépendante qui procède au contrôle préalable d'une communication des données de trafic aux autorités doit s'assurer que cette communication poursuit une des finalités pour laquelle elle peut avoir lieu et qu'elle respecte le principe de proportionnalité (cons. 156)

Pour le Centre de Connaissances,
(sé) Alexandra Jaspar, Directrice

ANNEXE I

Executive Summary

Le Ministre de la Justice, Monsieur Vincent Van Quickenborne a sollicité, le 7 mai 2021, l'avis de l'Autorité concernant un avant-projet de loi relatif à la collecte et à la conservation des données d'identification, de trafic et de localisation dans le secteur des communications électroniques et à leur accès par les autorités (ci-après « l'avant-projet de loi ») et un projet d'arrêté royal modifiant l'arrêté royal du 19 septembre 2013 portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques (ci-après « le projet d'arrêté »).

Cet avant-projet de loi vise à répondre à l'annulation de la loi du 29 mai 2016 « relative à la collecte et à la conservation des données dans le secteur des communications électroniques » par la Cour constitutionnelle. Le 21 avril 2021, la Cour constitutionnelle a, en effet, annulé cette loi du 29 mai 2016 qui reposait, dans son principe, sur une obligation de conservation généralisée et indifférenciée des données de trafic et de localisation des utilisateurs de moyens de communications électronique. Or la Cour constitutionnelle, dont la motivation renvoie largement à l'arrêt de la Cour de justice de l'Union européenne (CJUE) du 6 octobre 2020 (arrêt « Quadrature du Net »), juge que **l'obligation de conservation des données relatives aux communications électroniques doit être l'exception, et non la règle**. Dans son arrêt, la Cour constitutionnelle rappelle qu'*« il appartient au législateur d'élaborer une règlementation qui respecte les principes applicables en matière de protection des données à caractère personnel, à la lumière de la jurisprudence de la Cour de justice, et de tenir compte, le cas échéant, des précisions apportées par celle-ci en ce qui concerne les différents types de mesures législatives jugées compatible avec [la directive ePrivacy, lue à la lumière de la Charte des droits fondamentaux de l'Union européenne]* ».

L'avant-projet de loi cherche à mettre en place un système de conservation des métadonnées de communication qui respecte les exigences imposées par le droit européen, tel qu'il est interprété par la CJUE (pour une synthèse de ce système, voyez le tableau repris dans l'Annexe II). **Force est toutefois de constater que l'avant-projet de loi n'opère pas réellement le changement de perspective exigé par la jurisprudence de la CJUE et la CC**. En effet, l'Autorité constate, dans son avis, que l'avant-projet de loi entend imposer de nouvelles mesures de conservation des données de trafic et de localisation qui pourraient aboutir à réintroduire, *de facto*, des obligations de conservation généralisée et indifférenciée des données, tout en opérant une extension des possibilités d'accès à ces données. **Certes, la conservation de métadonnées peut être nécessaire pour garantir le droit à la sécurité de personnes qui est, comme le droit au respect de la vie privée et à la protection des données à caractère personnel, un droit fondamental consacré par la Constitution belge, la Convention européenne des droits de l'homme et la Charte des droits fondamentaux de l'Union européenne**. Le droit à la sécurité génère, en effet, des obligations positives, dans le chef de l'Etat,

d'adopter des mesures matérielles et procédurales permettant de lutter efficacement contre les infractions pénales commises contre les personnes à travers une enquête et des poursuites effectives. La CJUE reconnait la nécessité de procéder à une conciliation entre ces différents droits fondamentaux**. L'Autorité invite le législateur à prendre le temps de la réflexion et de l'analyse rigoureuse pour concilier, dans le respect de la jurisprudence européenne, les droits fondamentaux à la sécurité et à un recours effectif en cas d'infractions pénales portant atteinte à cette sécurité, d'une part, et les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, d'autre part**. L'Autorité insiste pour que le législateur adapte son avant-projet de loi pour que la loi qui sera votée respecte toutes les exigences imposées par la CJUE et la Cour constitutionnelle. Une nouvelle annulation par la Cour constitutionnelle de la loi serait de nature à entacher la confiance des citoyennes et les citoyens dans les institutions démocratiques. **Il est, dans cette perspective, tout à fait crucial de s'assurer que l'avant-projet de loi ne réintroduise pas, *de jure* ou *de facto*, une obligation de conservation généralisée et indifférenciée 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.** L'Autorité a émis, dans son avis, de très nombreuses remarques à propos de l'avant-projet de loi qui pointent les adaptations qui doivent y être apportées afin d'assurer la conformité de la règlementation en projet avec les exigences découlant du droit à la protection des données à caractère personnel tel qu'il est interprété par la CJUE.

Par ailleurs, **l'Autorité est inquiète de constater que l'avant-projet de loi prévoit d'obliger les opérateurs qui mettent en place un système d'encryptage à rendre possible les mesures d'interception légale**, en particulier l'identification de l'utilisateur final, le repérage et la localisation des communications non accessibles au public ainsi que les écoutes, la prise de connaissance et l'enregistrement des communications non accessibles au public. En effet, il existe, depuis les années 1990, un consensus dans la communauté scientifique pour considérer que l'insertion de « portes dérobées » (« backdoors ») dans les systèmes de cryptographie présente plus de risques pour la vie privée des personnes concernées et les intérêts supérieurs des Etats que d'avantages en termes de lutte contre la criminalité grave. **L'Autorité s'inquiète aussi de l'introduction d'obligations de collecte de données par des services, tels que des messageries encryptées, qui pour des raisons légitimes de sécurité et de protection de la vie privée ont jusqu'à présent évité de collecter ces données**.

ANNEXE II

Tableau récapitulatif des mesures de conservation préventive des données de trafic et de localisation

BASE LÉGALE	QUI DOIT CONSERVER ?	AUTORISATION OU OBLIGATION DE CONSERVATION DE DONNÉES	CATÉGORIES DE DONNÉES À CONSERVER	PRÉCISION CONCERNANT LES DONNÉES À CONSERVER	FINALITÉ INITIALE POURSUIVIE PAR LA CONSERVATION DE DONNÉES	AUTORITÉ(S) POUVANT ACCÉDER À CES DONNÉES & FINALITÉ(S) POUVANT JUSTIFIER CET ACCES
Art. 122§2 de la loi télécom (nouveau)	Tous les opérateurs	Autorisation	Données de trafic nécessaires à l'établissement des factures des abonnés ou celles qui sont nécessaires aux paiements d'interconnexion	Non – il n'y a pas de liste détaillée des données (ni dans la loi ni dans un AR) Mais l'opérateur doit informer les abonnées des données traitées	Établir les factures des abonnés et payer les interconnexions	Les autorités et les finalités listées à l'article 127/1 de la loi télécom
Art. 122§3 de la loi télécom (nouveau)	Tous les opérateurs	Autorisation, mais nécessité d'obtenir le consentement (au sens RGPD) de l'abonné préalablement au traitement	Données de trafic, y compris les données de localisation	Non – il n'y a pas de liste détaillée des données (ni dans la loi ni dans un AR) Mais l'opérateur doit informer les abonnées des données traitées	Assurer le marketing des services de communications électroniques propres et établir le profil d'utilisation de l'abonné ou de l'utilisateur final	Les autorités et les finalités listées à l'article 127/1 de la loi télécom
Art. 122§4 de la loi télécom	Tous les opérateurs	Obligation (nouveauté de l'avant-projet)	Données de localisation et d'autres des données de trafic nécessaires afin de	Pas de liste détaillée dans l'avant-projet, mais délégation facultative au Roi qui	Détecter et analyser une fraude présumée ou une utilisation	Les autorités et les finalités listées à l'article 127/1 de la loi télécom

(nouveau)			détecter et d'analyser une fraude présumée ou une utilisation malveillante présumée du réseau	peut – mais ne doit pas – déterminer les données à conserver sur pied de cette disposition	malveillante présumée du réseau	
Art. 122 § 4/1 de la loi télécom (nouveau)	Tous les opérateurs	Obligation (nouveauté de l'avant-projet)	Données de trafic nécessaires pour assurer la sécurité et le bon fonctionnement du réseau et des services de communications électroniques	Pas de liste détaillée dans l'avant-projet et pas de délégation au Roi pour déterminer les données à conserver	Assurer la sécurité et le bon fonctionnement du réseau et des services de communications électroniques, et en particulier détecter et analyser une atteinte potentielle ou réelle à cette sécurité, en ce compris identifier l'origine de cette atteinte	Les autorités et les finalités listées à l'article 127/1 de la loi télécom
Art. 123 de la loi télécom (nouveau)	Opérateurs de réseaux mobiles	Autorisation (nécessité d'obtenir le consentement de l'abonné dans certains cas)	Données de localisation autres que les données de trafic	Pas de liste détaillée dans l'avant-projet et pas de délégation au Roi pour déterminer les données à conserver	Bon fonctionnement et sécurité du réseau/service Détecter et analyser une fraude présumée ou une utilisation malveillante présumée du réseau Nécessaire pour fournir un service à valeur ajoutée (consentement nécessaire)	Les autorités et les finalités listées à l'article 127/1 de la loi télécom

Art. 126 de la loi télécom (nouveau)	Opérateurs qui offrent aux utilisateurs finaux des services de communications électroniques & opérateurs fournissant les réseaux de communications électroniques sous-jacents	Obligation	Données de souscription de l'abonné & données techniques nécessaires pour identifier l'utilisateur final, l'équipement terminal ou le service de communications électroniques employé, à l'exception des données qui sont liées à une seule communication électronique	Délégation au Roi pour déterminer les données précises à conserver Cf. nouveaux articles 3§1, 4§1, 5§1 et 6§1 de l'AR du 19/09/2013	Conservation pour les autorités et les finalités identifiées à l'article 127/1 de la loi télécom (reprises dans la colonne de droite)	Les autorités et les finalités listées à l'article 127/1 de la loi télécom
Art. 126/1 de la loi télécom (nouveau)	Opérateurs qui offrent aux utilisateurs finaux des services de communications électroniques & opérateurs fournissant les réseaux de communications électroniques sous-jacents	Obligation ciblée sur base de critères géographique	Les données relatives à l'accès et la connexion de l'équipement terminal au réseau et au service et à la localisation de cet équipement, y compris le point de terminaison du réseau Les données de communication, à l'exclusion du contenu, en ce compris leur origine et leur destination	Délégation au Roi pour déterminer les données précises à conserver Cf. nouveaux articles 3§2, 4§2, 5§2 et 6§2 de l'AR du 19/09/2013	Sauvegarde de la sécurité nationale Lutte contre la criminalité grave, Prévention de menaces graves contre la sécurité publique Sauvegarde des intérêts vitaux d'une personne physique	Les autorités et les finalités listées à l'article 127/1 de la loi télécom Mais l'accès à ces données n'est possible qu'à condition que cet accès poursuive l'une des finalités suivantes : la sauvegarde de la sécurité nationale, la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique et la sauvegarde des intérêts vitaux d'une personne physique.

			Les données des appels infructueux			
Art. 127 de la loi télécom (nouveau)	Tous les opérateurs	Obligation	Données nécessaires pour que les autorités qui sont habilitées à obtenir l'identité des abonnés des opérateurs puissent les identifier	Il n'y a pas de liste détaillée dans l'avant-projet, mais délégation facultative au Roi qui peut – mais ne doit pas – déterminer les données à conserver sur pied de cette disposition [L'AR du 19/9/2013 n'exécute pas cette disposition]	Conservation pour les autorités et les finalités identifiées à l'article 127/1 de la loi télécom (reprises dans la colonne de droite)	Les autorités et les finalités listées à l'article 127/1 de la loi télécom

Le nouvel article 127/1 de la loi télécom détermine les autorités qui peuvent accéder aux données conservées par les opérateurs télécom en exécution de la loi télécom et les finalités pouvant justifier cet accès. Il s'agit des autorités et des finalités suivantes :

1° les autorités répressives pour la prévention, la recherche, la détection et la poursuite d'infractions ;

2° les services de renseignement et de sécurité pour l'exercice de leurs missions légales ;

3° les autorités chargées d'apporter de l'aide aux personnes ;

4° l'IBPT pour l'exercice de ses missions légales ;

5° les autorités compétentes pour l'examen d'une défaillance de la sécurité du réseau ou du service

L'accès aux données se fait aux conditions prévues par les lois organiques des différentes autorités listées à l'article 127/1 de la loi télécom.