



Avis n° 33/2015 du 9 septembre 2015

Objet : demande d'avis concernant l'avant-projet de loi relative à la collecte et à la conservation des données dans le secteur des communications électroniques (CO-A-2015-040)

La Commission de la protection de la vie privée (ci-après "la Commission") ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après la "LVP"), en particulier l'article 29 ;

Vu la demande d'avis du Ministre de la Justice, Monsieur Koen Geens, reçue le 28/07/2015 ;

Vu le rapport du Monsieur Willem Debeuckelaere, Président ;

Émet, le 9 septembre 2015, l'avis suivant :

A. INTRODUCTION

1. Le 27 juillet 2015, le Ministre de la Justice a demandé à la Commission d'émettre un avis en extrême urgence concernant l'avant-projet de loi relative à la collecte et à la conservation des données dans le secteur des communications électroniques (ci-après "l'avant-projet de loi").
2. L'extrême urgence est dûment motivée. La Commission émettra dès lors ci-après un avis en extrême urgence concernant l'avant-projet susmentionné, en tenant compte des informations dont elle dispose.

B. ANTÉCÉDENTS

3. Le 2 juillet 2008, la Commission avait déjà émis un avis (avis n° 24/2008) *relatif à l'avant-projet de loi modifiant l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques et au projet d'arrêté royal fixant les données à conserver en application de l'article 126 de la loi du 13 juin 2005* (ci-après "la LCE"), *ainsi que les conditions et la durée de conservation de ces données*. L'avis qu'elle avait émis à l'époque était défavorable. Ensuite, la Commission a à nouveau émis un avis le 1^{er} juillet 2009 (avis n° 20/2009) *relatif à l'avant-projet de loi et au projet d'arrêté royal en matière de rétention de données et au projet d'arrêté royal relatif à l'obligation de collaboration*. Ce dernier avis était favorable, moyennant le respect de plusieurs conditions.
4. La Directive 2006/24/CE¹ appelée "Directive conservation de données" a ensuite été transposée en droit belge par la loi du 30 juillet 2013 *portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90decies du Code d'instruction criminelle*.
5. La Directive 2006/24/CE a toutefois été invalidée par la Cour européenne de Justice² le 8 avril 2014. La Cour a déclaré que la Directive représentait une ingérence particulièrement importante dans les droits consacrés par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne. La Cour a estimé que cette conservation de données répondait bel et bien à une finalité d'intérêt général et qu'elle constituait un instrument utile dans le cadre d'instructions. Toutefois, en raison de cette importante ingérence, la Directive

¹ 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*.

² Cour européenne de Justice, 8 avril 2014, C-293/12 et C-594/12.

doit établir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant un minimum d'exigences de sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données.

6. La Cour a estimé que la Directive n'offrait pas suffisamment de garanties et s'est basée pour ce faire sur les arguments suivants : 1) la Directive concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, sans distinction, même si leur comportement ne laisse supposer aucun lien avec la criminalité grave et même si elles sont soumises au secret professionnel ; 2) il n'y a aucune restriction ni aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure ; l'accès n'est en outre subordonné à aucun contrôle préalable effectué par une instance judiciaire ou par une entité administrative indépendante ; 3) la durée de conservation n'établit aucune distinction entre les catégories de données en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées et elle varie entre six et vingt-quatre mois, sans qu'il soit précisé que la détermination de la durée de conservation doit être fondée sur des critères objectifs afin de garantir que celle-ci est limitée au strict nécessaire ; 4) la Directive ne garantit pas que les fournisseurs de services de communications électroniques offrent un niveau particulièrement élevé de protection et de sécurité par des mesures techniques et organisationnelles et elle ne garantit pas non plus la destruction irrémédiable des données au terme de la durée de conservation de celles-ci ; en outre, la Directive n'impose pas que les données soient être conservées sur le territoire de l'UE, de manière à permettre le contrôle par une autorité indépendante du respect des exigences de protection et de sécurité.
7. Le 11 juin 2015, la Cour constitutionnelle a dès lors invalidé la loi susmentionnée du 30 juillet 2013 pour violation des articles 10 et 11 de la Constitution, lus conjointement avec les articles 7 et 8 de la Charte de l'UE. La Cour s'est en grande partie basée à cet égard sur l'argumentation précitée de la Cour européenne de Justice, étant donné qu'elle dénonce en premier lieu le large champ d'application de la loi, à savoir le traitement de l'ensemble des données de toutes les personnes. Une deuxième critique porte sur l'absence de condition matérielle ou procédurale pour l'accès par les autorités aux données conservées. Enfin, la Cour juge problématique qu'en ce qui concerne la période de conservation, la loi n'établisse aucune distinction entre les catégories de données en fonction de leur utilité ou des personnes concernées.

C. EXAMEN DE LA DEMANDE D'AVIS

C.1. Remarques générales

8. Tout d'abord, il convient de rappeler que l'avant-projet de loi ne porte pas sur *le contenu* de certaines communications électroniques. Il vise les données d'identification de l'utilisateur, les données relatives aux services de communication fournis à un abonné, à l'accès au terminal et à la connexion de ce terminal avec les réseaux, avec le service ainsi que les données relatives à la localisation de ce terminal et les données de communication, à l'exception du contenu.
9. En vertu de l'arrêt susmentionné de la Cour européenne de Justice, la conservation des données prescrite par la Directive 2006/24/CE peut effectivement répondre à une finalité d'intérêt général, à savoir contribuer à la sécurité publique en luttant contre la criminalité grave, à propos de quoi la Cour observe que chacun a droit non seulement à la liberté mais aussi à la sécurité sûreté. Toutefois, une ingérence dans la vie privée des individus aussi poussée nécessite de prévoir des garanties suffisantes et être adéquatement motivée quant à la nécessité de la conservation des données concernées pour garantir effectivement la sûreté publique. L'Exposé des Motifs³ explique en détail la nécessité d'une telle obligation de conservation dans le cadre d'une enquête pénale ou de renseignement.
10. Enfin, on peut faire remarquer que les fournisseurs de services de communications électroniques conservent déjà sans aucune obligation certaines de ces données à des fins commerciales conformément à l'article 122 de la loi du 13 juin 2005, notamment à des fins de facturation. Ces données sont aujourd'hui utilisées pour les finalités de l'enquête pénale ou du renseignement, dans les conditions prévues par ces cadres légaux.
11. Il n'appartient pas à la Commission d'apprécier la manière dont on doit tenir compte en pratique des arrêts susmentionnés pour la rédaction de la nouvelle réglementation. Toutefois, certains aspects des arrêts en question lui paraissent difficilement applicables, en particulier la distinction en fonction des personnes, périodes temporelles et/ou zones géographiques. À cet égard, on peut renvoyer à l'argumentation reprise dans l'Exposé des Motifs⁴. Cependant, comme indiqué dans l'Exposé des Motifs⁵, aucun des deux arrêts ne conclut qu'un seul des quatre éléments suffit à constituer une violation du principe de

³ Exposé des Motifs, pp. 2-7.

⁴ Exposé des Motifs, pp. 7-11.

⁵ Exposé des Motifs, pp. 10-11.

proportionnalité. Si un élément déterminé des arrêts ne peut pas être retenu, il faut compenser cet élément par un régime plus strict sur les autres aspects.

12. Pour la Commission, les principaux aspects de la réglementation sur la conservation de données sont la limitation dans le temps, les restrictions spécifiques en termes d'accès et d'utilisation ainsi que les mesures de sécurité techniques et organisationnelles incluant la destruction des données conservées, une fois la durée de conservation légale expirée. Il convient également de tenir compte des droits des personnes qui sont liées par le secret professionnel. Enfin, un contrôle parlementaire est nécessaire, ainsi qu'un contrôle par des instances indépendantes. Pour ce dernier aspect, il est essentiel que les données soient conservées en Belgique. Ces différents points sont repris ci-après dans le commentaire des articles de l'avant-projet de loi.

C.2. Commentaire des articles

13. La Commission va procéder ci-après au commentaire des articles de l'avant-projet de loi, en se limitant aux articles pour lesquels elle a des remarques à formuler.

Article 4

14. Conformément à l'Exposé des Motifs, la nouvelle version de l'article 126 de la LCE est prise sur la base de l'article 15.1 de la Directive 2002/58/CE *concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques*. Cet article 15.1 permet aux États membres d'adopter des mesures réglementaires prévoyant la conservation de données pendant une durée limitée lorsque c'est justifié par un des motifs énumérés dans l'article en question, à savoir pour sauvegarder la sûreté de l'État, la défense et la sécurité publique, ou pour assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées de systèmes de communications électroniques, tels que visés à l'article 13, alinéa 1 de la Directive 95/46/CE.
15. Cet article ne s'applique pas aux fournisseurs et revendeurs au sens de l'article 9, §§ 5 et 6 de la LCE. Cela correspond à la demande requête formulée par la Commission dans ses précédents avis.
16. Le paragraphe 1^{er} précise que les données ne doivent être conservées par les fournisseurs et opérateurs concernés que pour autant que ces données soient générées ou traitées par eux

dans le cadre de la fourniture des services de communications concernés. Lorsque ce n'est pas le cas, il n'y a pas d'obligation de les conserver. Il est précisé que cet article ne porte pas sur le contenu de la communication.

17. Le paragraphe 2 énumère ensuite les autorités pouvant obtenir les données conservées en vertu de l'article 126. La Commission accueille favorablement ce paragraphe qui indique beaucoup plus clairement que par le passé quelles autorités peuvent accéder à quelles données déterminées et pour quelles finalités.
18. Il est en outre précisé que les fournisseurs et opérateurs ne peuvent pas utiliser les données conservées en vertu du paragraphe 3 pour d'autres finalités. Ces données ne pourront dès lors pas être utilisées pour des finalités commerciales. Toute violation de cette disposition est sanctionnée conformément à l'article 7 de l'avant-projet de loi.
19. Le paragraphe 3 prévoit ensuite un délai de conservation spécifique, variant de 2 à 12 mois. Une des remarques de la Cour constitutionnelle concernait en effet le fait qu'en ce qui concerne la durée de conservation des données, aucune distinction n'était établie entre les catégories de données en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi. L'avant-projet tient compte de cette remarque en introduisant une distinction sur la base de quatre catégories de données. Dans ses précédents avis, la Commission avait déjà indiqué qu'un délai de 12 mois était actuellement suffisant. À cet égard, l'évaluation proposée est également importante (voir le point 23), où le délai pourrait être révisé à la hausse ou à la baisse, si cela s'avérait nécessaire. Enfin, on peut renvoyer aux articles 8 et 9 de l'avant-projet de loi, où une différenciation des délais est prévue pour la collecte de données (voir à ce sujet les points 26-30).
20. Le paragraphe 3 dispose en outre que le Roi fixera les données à conserver par catégorie, ainsi que les exigences auxquelles ces données doivent satisfaire. La Commission constate que dans l'avant-projet de loi, les catégories de données à conserver sont définies plus clairement. La mise en œuvre par le biais d'un arrêté royal pourra être suivie, sachant que le fonctionnement de l'avant-projet de loi fera l'objet d'une évaluation (voir ci-après le point 23) et que l'arrêté royal devra être promulgué après délibération en Conseil des Ministres et après avis de la Commission et de l'Institut belge des services postaux et des télécommunications, ci-après "l'IBPT".

21. Le paragraphe 4 définit les mesures de sécurité et de protection à prévoir par les opérateurs et fournisseurs. Ce paragraphe reprend d'une part certaines mesures de sécurité qui existaient déjà dans la loi annulée et ajoute d'autre part des mesures supplémentaires.
22. Les données conservées doivent faire l'objet de mesures de sécurité techniques et organisationnelles appropriées afin d'être sécurisées. Les données doivent être détruites de tout support à l'issue de la période de conservation, sans préjudice des articles 122 et 123 de la LCE. Toute violation de cette disposition est sanctionnée conformément à l'article 7 de l'avant-projet de loi. Une donnée déterminée ne doit pas être détruite à l'issue de la période de conservation prévue pour l'article 126 de la LCE uniquement si elle doit encore être conservée sur la base de l'article 122 ou 123 de la LCE. Dans ce cas, elle doit par contre être détruite à l'issue du délai de conservation prévu pour les articles 122 ou 123. Les nouvelles mesures de sécurité reprises au paragraphe 4 disposent que les données doivent être conservées sur le territoire de l'Union européenne, conformément à l'arrêt de la Cour européenne de Justice. Dès leur enregistrement, les données conservées doivent être rendues illisibles et inutilisables pour toute personne non autorisée à y accéder. Enfin, il convient d'instaurer une traçabilité de l'exploitation des données conservées à l'aide d'un journal. Dans le cadre de leur mission de contrôle, l'IBPT et la Commission peuvent exiger la consultation de ce journal. Le contenu de ce journal est fixé par arrêté royal, après avis de la Commission et de l'IBPT. La Commission constate que les mesures susmentionnées représentent une amélioration des mesures de sécurité et de protection que les opérateurs et les fournisseurs doivent prévoir. Elle note également qu'elle sera responsable, conjointement avec l'IBPT, du contrôle du respect des dispositions légales relatives à la conservation de données. Il est recommandé de prévoir un protocole de collaboration entre les deux services afin de garantir un contrôle efficace. Il est préférable que l'élaboration d'un tel protocole soit prévue dans l'avant-projet de loi.
23. Les paragraphes 5 et 6 prévoient une double évaluation de la loi, comme la Commission l'avait également déjà demandé dans ses précédents avis. D'une part, une évaluation approfondie unique doit avoir lieu deux ans après l'entrée en vigueur du futur arrêté royal portant exécution de l'article 126, § 3. D'autre part, l'avant-projet de loi prévoit également un rapport annuel à la Chambre des représentants.

Article 5

24. Cet article introduit un nouvel article 126/1 dans la loi du 13 juin 2005 qui traite de la constitution d'une Cellule de coordination au sein de chaque opérateur ou fournisseur. Cette cellule est chargée de fournir aux autorités légalement habilitées les données conservées en vertu des articles 122, 123 et 126 de la LCE. Chaque membre de cette cellule doit faire l'objet d'un avis de sécurité positif et ne pas avoir fait l'objet d'un refus du Ministre de la Justice. Les membres sont soumis au secret professionnel. Les fournisseurs et opérateurs doivent en outre désigner un ou plusieurs préposés à la protection des données, lesquels – contrairement à la loi annulée – ne peuvent pas faire partie de la Cellule de coordination. La Commission adhère à cette mesure étant donné qu'elle permet en effet au préposé de contrôler le fonctionnement de la cellule en toute indépendance et en toute impartialité. Il est encore précisé que l'exercice de ses missions ne peut entraîner de désavantages au préposé et qu'il doit avoir la possibilité de communiquer directement avec le management ou le comité de direction.

Article 7

25. L'avant-projet de loi insère une disposition pénale additionnelle complétant les dispositions pénales déjà existantes dans le Code pénal concernant le hacking externe et interne. L'hypothèse qu'une personne travaillant au sein de la Cellule de coordination n'outrepasse pas son pouvoir d'accès mais fasse ultérieurement un usage non autorisé par la loi des données qu'elle a obtenues d'une manière légale et justifiée n'est pas encore couverte par la loi. C'est la raison pour laquelle l'avant-projet de loi introduit une nouvelle incrimination prévoyant bel et bien ce cas de figure.

Article 8

26. Cet article ajoute un alinéa 4 au § 1^{er} de l'article 46*bis* du Code d'instruction criminelle, introduisant ainsi une différenciation de l'accès aux données à l'article 46*bis*. Pour certaines infractions de moindre gravité, ces données peuvent uniquement être requises pour une période de six mois préalable à la décision du procureur du Roi. La Commission constate que cette solution répond aux critiques formulées par la Cour européenne de Justice et la Cour constitutionnelle et constitue une amélioration par rapport à la situation antérieure.

Article 9

27. Cet article comporte un certain nombre de modifications à l'article 88*bis* du Code d'instruction criminelle qui prévoient une différenciation en ce qui concerne les délais pour la demande de données. D'après l'Exposé des Motifs, ces modifications sont de trois ordres :
- limitation du champ d'application et des délais dans lesquels les données peuvent être demandées ;
 - protection du secret professionnel des avocats et des médecins ;
 - adaptations terminologiques et adaptations à l'évolution constante de la technologie.
28. Tout d'abord, l'article 9, 1^o introduit une exigence de proportionnalité en limitant le champ d'application de l'article 88*bis* aux infractions pour lesquelles il existe des indices sérieux que ces infractions peuvent donner lieu à une peine d'emprisonnement correctionnel principal d'un an ou à une peine plus lourde. Ensuite, l'article 9, 6^o prévoit que le juge d'instruction ne peut recourir à la totalité du délai de conservation de 12 mois que pour certaines infractions. Pour d'autres infractions, il ne peut requérir les données que pour une période de six mois préalable à l'ordonnance. La Commission constate que ces exigences de proportionnalité constituent une amélioration par rapport à la situation antérieure
29. Enfin, l'article 9, 7^o prévoit une mesure d'exception pour certaines catégories professionnelles, en vue de protéger leur secret professionnel. Cela représente aussi une amélioration par rapport à la situation antérieure. La Commission remarque toutefois que l'avant-projet de loi n'a pas repris la catégorie professionnelle des journalistes dans cette mesure d'exception, ce qui était par contre le cas à l'article 12 de l'avant-projet de loi. La Commission demande dès lors d'également appliquer cette mesure d'exception aux journalistes.
30. L'article 46*bis* du Code d'instruction criminelle prévoit une motivation formelle par le procureur du Roi, cette motivation devant refléter la proportionnalité en tenant compte de la vie privée et de la subsidiarité à tout autre devoir d'enquête. L'article 88*bis* comporte une disposition identique pour le juge d'instruction.

Article 12

31. Cet article fait partie du chapitre IV de l'avant-projet, qui traite des dispositions modifiant la *loi organique des services de renseignement et de sécurité* du 30 novembre 1998. Le texte prévoit de nouvelles garanties supplémentaires pour l'utilisation de méthodes spécifiques en imposant de nouvelles mentions devant figurer dans la décision du dirigeant du service, dont les circonstances de fait qui justifient la méthode spécifique, la motivation en matière de subsidiarité et de proportionnalité et le lien entre la cible de la méthode et la menace potentielle. Il instaure également une procédure de protection particulière pour les médecins, les avocats et les journalistes.

Article 13

32. Afin de répondre aux critiques de la Cour européenne de Justice et de la Cour constitutionnelle, cet article aussi introduit une différenciation au niveau des délais dans lesquels les données de trafic et de localisation peuvent être demandées. La Commission constate que ces exigences de proportionnalité représentent une amélioration par rapport à la situation antérieure.

PAR CES MOTIFS,

la Commission

émet un avis *favorable* concernant le présent avant-projet de loi, à condition qu'il soit tenu compte des remarques formulées aux points 22 et 29.

L'Administrateur f.f.,

Le Président,

(sé) An Machtens

(sé) Willem Debeuckelaere