Avis n° 24 /2008 du 2 juillet 2008

Objet : avis 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, ainsi que les conditions et la durée de conservation de ces données (A/2008/024)

La Commission de la protection de la vie privée ;

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 pour l'Entreprise et la Simplification, reçue le 23/05/2008 ;

Vu le rapport de Madame Anne Vander Donckt ;

Émet, le 02/07/2008, l'avis suivant :

A. INTRODUCTION

1. Le 23 mai 2008, le Ministre pour l'Entreprise et la Simplification a demandé à la Commission d'émettre un avis concernant les propositions visant à transposer la Directive européenne 2006/24/CE *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. Il s'agit plus précisément d'un avant-projet de loi modifiant l'article 126 de la loi du 13 juin 2005 *relative aux communications électroniques* (ci-après "l'avant-projet de loi"), et d'un projet d'arrêté royal fixant les données à conserver en application de l'article 126 de la loi du 13 juin 2005, ainsi que les conditions et la durée de conservation de ces données (ci-après "le projet d'arrêté royal"). La Commission émettra dès lors ci-après un avis sur ces projets, en tenant compte des informations dont elle dispose.

B. LÉGISLATION APPLICABLE

3. Tout d'abord, on peut faire référence à la Directive 2006/24/CE. Étant donné que des données à caractère personnel sont traitées, la LVP ainsi que la loi du 13 juin 2005 *relative aux communications électroniques* (ci-après "la LCE") sont d'application. Enfin, il convient de mentionner l'arrêté royal du 9 janvier 2003 *portant exécution des articles 46bis, § 2, alinéa 1er, 88bis, § 2, alinéas 1er et 3, et 90quater, § 2, alinéa 3, du code d'instruction criminelle ainsi que de l'article 109ter, E, § 2, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques* (ci-après "l'arrêté royal du 9 janvier 2003").

C. ANTÉCÉDENTS

4. Par le passé, plusieurs États membres européens ont légiféré sur la conservation de données par les fournisseurs de services en vue de la prévention, de la recherche, de la détection et de la poursuite d'infractions pénales. Lesdites dispositions nationales varient considérablement. Les disparités législatives et techniques existant entre les dispositions nationales relatives à la conservation de données en vue de la prévention, de la recherche, de la détection et de la poursuite d'infractions pénales constituent des entraves au marché intérieur des communications électroniques dans la mesure où les fournisseurs de services doivent satisfaire à des exigences différentes pour ce qui est des types de données relatives au trafic et à la localisation à conserver ainsi que des conditions et des durées de conservation.

5. Dans ses conclusions, le Conseil européen "Justice et affaires intérieures" du 19 décembre 2002 souligne qu'en raison de l'accroissement important des possibilités qu'offrent les communications électroniques, les données relatives à l'utilisation de celles-ci sont particulièrement importantes et constituent donc un instrument utile pour la prévention, la recherche, la détection et la poursuite d'infractions pénales, notamment de la criminalité organisée. Dans sa déclaration du 25 mars 2004 sur la lutte contre le terrorisme, le Conseil européen a chargé le Conseil "Justice et affaires intérieures" d'envisager des propositions en vue de l'établissement de règles relatives à la conservation, par les fournisseurs de services, des données relatives au trafic des communications. Le 13 juillet 2005, le Conseil européen a réaffirmé, dans sa déclaration condamnant les attentats terroristes de Londres, la nécessité d'adopter dans les meilleurs délais des mesures communes relatives à la conservation de données concernant les télécommunications.

6. **Les finalités de la Directive 2006/24/CE consistent dès lors à harmoniser les obligations imposées aux fournisseurs en matière de conservation de certaines données et à garantir que ces données soient disponibles à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne**.

7. Le Groupe 29[1] a précisé dans son avis n° 3/2006 concernant la Directive 2006/24 qu'afin de transposer uniformément ses dispositions et de respecter les conditions de l'article 8 de la CEDH, les États membres devraient mettre en place des garanties spécifiques suffisantes, comprenant au minimum les garanties suivantes :

   - description de la finalité : le terme "infraction grave" devrait être clairement défini et encadré ;
   - limitation de l'accès : les données devraient être mises à la disposition des seuls services répressifs expressément désignés ;
   - données limitées au minimum ;
   - pas d'exploration des données ;
   - contrôle indépendant de l'autorisation d'accès ;

[1] Ce groupe de travail a été établi en vertu de l'article 29 de la Directive 95/46/CE et est un organe consultatif indépendant sur la protection des données et de la vie privée. Ses missions sont définies à l'article 30 de la Directive 95/46/CE et à l'article 15 de la Directive 2002/58/CE.

-
- séparation des systèmes ;
- mesures de sécurité ;
- finalité de la conservation des données par les fournisseurs.
-

D. EXAMEN DE LA DEMANDE D'AVIS

D.1. COMPARAISON DE L'ACTUEL ARTICLE 126 DE LA LCE AVEC LE NOUVEL AVANT-PROJET

8. L'actuel article 126 de la LCE est formulé comme suit : "*§ 1er. Par arrêté délibéré en Conseil des Ministres, le Roi fixe, sur proposition du Ministre de la Justice et du ministre et après avis de la Commission pour la protection de la vie privée et de l'Institut, les conditions dans lesquelles les opérateurs enregistrent et conservent les données de trafic et les données d'identification d'utilisateurs finals en vue de la poursuite et la répression d'infractions pénales, en vue de la répression d'appels malveillants vers les services d'urgence et en vue de 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.*

   § 2. Les données à conserver ainsi que la durée de la conservation, qui en matière de service téléphonique accessible au public ne peut ni être inférieure à douze mois ni dépasser trente-six mois, sont déterminées par le Roi dans un arrêté délibéré en Conseil des ministres, après avis de la Commission pour la protection de la vie privée et de l'Institut.

   Les opérateurs font en sorte que les données reprises au § 1er soient accessibles de manière illimitée de Belgique."

9. L'arrêté royal dont il est question au § 2 n'a jamais été adopté. L'actuel article 126 de la LCE s'applique aux opérateurs et non aux fournisseurs ou aux revendeurs prévus à l'article 9, §§ 5 et 6 de la LEC. Sont ainsi visés par exemple[2] les réseaux ou services destinés à être utilisés par les membres d'un groupe d'entreprises, un réseau d'une université, d'une banque et de ses agents, ... Dans l'avant-projet de loi, les fournisseurs et les revendeurs sont bel et bien repris à l'article 126 de la LCE. L'avant-projet de loi ajoute également les données de localisation à l'actuel article 126 de la LCE.

[2] Voir la Chambre des représentants de Belgique, justification des amendements du projet de loi portant des dispositions diverses, Doc. 51, 2873/002.

10. Dans son avis n° 08/2004[3], la Commission a notamment déclaré ce qui suit concernant l'actuel article 126 de la LCE :

"***La Commission rappelle les observations déjà formulées dans son avis 33/99 du 13 décembre 1999 et réitérées au niveau européen à plusieurs reprises par le groupe des commissaires européens à la protection des données[4], quant à la compatibilité d'une rétention a priori des données de communication avec les principes fondamentaux de protection des données à caractère personnel***.

La Commission avait ainsi rappelé que "ni les textes internationaux (...), ni la loi du 8 décembre 1992 (principes de proportionnalité, durée limitée, ...) n'autorisent les méthodes de surveillance globale indépendamment d'instructions relatives à des infractions particulières (si l'on excepte le cas très particulier de la recherche proactive, qui est strictement encadrée. La Commission se référait encore à la jurisprudence de la Cour européenne des droits de l'homme[5] "qui conduit à proscrire les mesures de surveillance exploratoire ou générale des télécommunications mises en œuvre sur une grande échelle. Ainsi, il ne pourrait être question d'obliger un fournisseur d'accès à enregistrer systématiquement tous les appels en provenance de ses clients mais uniquement lorsqu'une instruction est ordonnée vis-à-vis d'une personne en particulier. Il ne pourrait non plus être question de contraindre un fournisseur d'accès à tenir un log book des accès susceptibles de conforter l'instruction."

D.2. IMPLICATIONS PRATIQUES

11. Les présentes dispositions auront un impact important sur la gestion de l'entreprise, non seulement pour les grands opérateurs connus tels que par exemple Belgacom, Mobistar ou Telenet, mais également au sein d'une entreprise ou d'une PME qui prévoit un accès Internet et un service de courriers électroniques pour leurs travailleurs. Dans la version actuelle du projet, même un réseau domestique ne semble pas exclu, si on le met à disposition d'invités par exemple. À l'avenir, ils seront tenus de conserver et d'enregistrer les données demandées

---

[3] Avis n° 08/2004 du 14 juin 2004 *sur l'avant-projet de loi relatif aux communications électroniques*.

[4] Recommandation n° 3/99 du 7 septembre 1999 *relative à la préservation des données de trafic par les fournisseurs de services Internet pour le respect du* droit ; Avis 5/2002 du 11 octobre 2002 *sur la Déclaration des Commissaires européens à la protection des données adoptée lors de la conférence internationale de Cardiff du 9-11 septembre 2002, relative à la conservation systématique et obligatoire des données de trafic des télécommunications : "Lorsque des données de trafic doivent être conservées, [la] nécessité doit être démontrée, la période de conservation doit être aussi courte que possible et cette pratique doit être clairement établie par la loi, de façon à prévenir tout accès illégal ou tout autre forme d'abus. La conservation systématique de tout type de données de trafic pour une période d'un an ou plus serait clairement disproportionnée et par conséquent inacceptable."*

[5] Arrêts Klass et Malone.

pendant 24 mois ou plus. Ils doivent aussi satisfaire à des mesures de sécurité péremptoires, dont la création d'une 'Cellule de coordination de la Justice' et la nomination de préposés à la protection des données à caractère personnel. En outre, ils doivent immédiatement pouvoir mettre les données conservées à la disposition des demandeurs. Tout cela semble difficilement réalisable en pratique, d'autant que les réseaux visés à l'article 9, §§ 5 et 6 de la LCE ne doivent pas faire de déclaration auprès de l'IBPT et qu'il est par conséquent difficile d'effectuer par exemple un contrôle du respect des mesures de sécurité nécessaires par ces réseaux. Ils doivent également tenir compte des réglementations existantes en matière de protection de la vie privée, comme par exemple la CCT n° 81 du 26 avril 2002 concernant le contrôle de l'utilisation d'Internet et du courrier électronique sur le lieu de travail. Ces réglementations sont en contradiction flagrante avec ce que l'avant-projet de loi prévoit pour les fournisseurs visés à l'article 9, §§ 5 et 6 de la LCE. Enfin, il faut préciser à cet égard que la Directive 2006/24 ne vise que les services de communications électroniques ou les réseaux de communications **publics** et donc pas les fournisseurs visés à l'article 9, §§ 5 et 6 de la LCE.

12. En outre, il convient de signaler que les dispositions de la directive ont été rédigées en tenant notamment compte des remarques des opérateurs de télécommunications en matière de modalités techniques et pratiques d'enregistrement, comme les données à conserver. La Commission se demande dès lors dans quelle mesure le projet d'arrêté royal tient compte des possibilités techniques des opérateurs, certainement en ce qui concerne les données à conserver qui ne sont pas prévues dans la directive. La consultation du secteur par l'IBPT[6], récemment clôturée, pourra probablement fournir plus de précisions à ce sujet.

D.3. PRATIQUE ACTUELLE

13. Actuellement, il existe déjà un règlement détaillé concernant l'identification de numéros de téléphone (article 46*bis* du Code d'instruction criminelle, ci-après 'CIC') et le repérage ou la localisation de (télé)communications privées (article 88*bis* du CIC).

14. L'article 46*bis* du CIC octroie au procureur du Roi la compétence de requérir les données d'identification des services de télécommunication auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée. Ainsi, on peut vérifier quels numéros de téléphone sont liés à une personne déterminée. À l'inverse, au départ du numéro de téléphone que l'on a trouvé quelque part, on peut également demander quel abonné

[6] Consultation réalisée par le Conseil de l'IBPT à la demande du Ministre pour l'Entreprise et la Simplification du 27 mai 2008 concernant la transposition de la Directive 2006/24, délai de réponse jusqu'au 16 juin 2008 inclus.

ou utilisateur habituel y est associé[7]. L'article 46*bis*, § 2 du CIC stipule que "*Chaque opérateur (...) qui est requis de communiquer les données visées au paragraphe premier, donne au procureur du Roi (...) les données qui ont été demandées dans un délai à fixer par le Roi*". L'arrêté royal du 9 janvier 2003 a exécuté cette disposition.

15. Pour le repérage et la localisation, une ordonnance du juge d'instruction est requise. Il s'agit (1) du repérage de données d'appel des moyens de télécommunication desquels ou vers lesquels certains appels sont ou ont été passés et (2) de la localisation de l'origine ou de la destination de la télécommunication. Cela permet de localiser des personnes participant à une conversation par GSM, notamment via des liaisons satellites et en déterminant l'antenne émettrice[8]. L'article 88*bis* du CIC stipule que "*chaque opérateur (...) communique les informations qui ont été demandées dans un délai à fixer par le Roi (...)*". Les modalités de la collaboration technique sont également déterminées par le Roi. L'arrêté royal du 9 janvier 2003 a exécuté cette disposition.

16. Il n'est pas clair de savoir pour quelle raison les articles susmentionnés et l'arrêté royal du 9 janvier 2003 qui les exécute ne suffiraient pas pour l'information judiciaire et l'instruction. Quelle est la nécessité d'une obligation de conservation telle que prévue par l'avant-projet de loi ? Quel est l'impact de l'avant-projet de loi et du projet d'arrêté royal sur les articles 46*bis* et 88*bis* du CIC susmentionnés, ainsi que sur l'arrêté royal du 9 janvier 2003 ? Les projets de textes ne nous renseignent pas à ce sujet.

D.4. DISCUSSION DES ARTICLES DE L'AVANT-PROJET DE LOI

ARTICLE 2

17. L'article 2 remplace l'actuel article 126 de la LCE. Le § 1er de l'article 2 de l'avant-projet de loi est libellé comme suit :

"*Sans préjudice 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, les opérateurs, ainsi que les fournisseurs et revendeurs visés à l'article 9, §§ 5 et 6, conservent les données de trafic, de localisation et les données d'identification d'utilisateurs finals qui sont générées ou traitées par eux lors de la fourniture de réseaux ou de services de communications électroniques, et ce en vue :*

[7] VAN DEN WYNGAERT, C., "Strafrecht, strafprocesrecht en internationaal strafrecht, in hoofdlijnen", Maklu, 2006, p. 979.

[8] VAN DEN WYNGAERT, C., op. cit., p. 979-980.

a) de la recherche, de la poursuite et de la répression d'infractions pénales ;

b) de la répression d'appels malveillants vers les services d'urgence ;

c) de 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."

18. Comme déjà précisé au point 9 susmentionné, l'article 2 de l'avant-projet de loi ne mentionne pas uniquement les opérateurs mais également les fournisseurs et les revendeurs visés à l'article 9, §§ 5 et 6 de la LCE. Ainsi, les entités qui étaient auparavant visées dans la LCE par deux dispositions distinctes en matière de conservation de données sont regroupées en une seule disposition (le nouvel article 126).

19. Dans l'ancien article 126 de la LCE, ce qui précède était déjà prévu pour un opérateur, à présent les fournisseurs et les revendeurs mentionnés à l'article 9, §§ 5 et 6 de la LCE viennent également s'y ajouter. L'article 9, § 7 prévoyait qu'ils devaient également enregistrer et conserver les données pour les finalités a) et b) mais pas pour la finalité c). Dorénavant, c'est le cas. Par fournisseurs et revendeurs, il faut par exemple entendre le réseau interne d'un groupe d'entreprises. Toutefois, ceux-ci ne sont pas visés par la Directive 2006/24/CE qui, conformément à l'article 3, s'applique uniquement aux fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications dans le cadre de la fourniture des services de communication concernés.

20. La raison de ne pas mentionner les fournisseurs et les revendeurs dans l'actuel article 126 de la LCE mais bien dans l'article 9, § 7 de la LCE peut être retrouvée dans la justification donnée pour l'un des amendements[9] du projet de loi portant des dispositions diverses concernant les §§§ 5, 6 et 7 : "*Par ailleurs, il est nécessaire de prévoir une collaboration avec les autorités judiciaires. L'obligation de coopération telle qu'elle est prévue pour les opérateurs (avec notamment l'obligation de désigner une personne de contact avec les autorités judiciaires, disponible 7 jours sur 7 et 24 heures sur 24) n'est également pas opportune à cet égard. Par conséquent, la possibilité de définir des modalités relatives à la conservation de données et à la coopération avec les autorités judiciaires dans un arrêt d'exécution est créée.*" Ce passage démontre que l'on ne peut pas assimiler ainsi les fournisseurs et les revendeurs dont il est question à l'article 9, §§ 5 et 6 de la LCE à un opérateur au sens de l'article 2, 11° de la LCE. On ne voulait certainement pas déclarer applicable de la même façon aux fournisseurs et aux revendeurs la lourde procédure de collaboration avec les autorités judiciaires, telle que prévue dans l'arrêté royal du 9 janvier 2003. Il est dès lors étrange que cela se produise à présent, en

[9] Voir le projet de loi portant des dispositions diverses, 9 juin 2006, doc. 51, 2518/007, page 4.

rendant l'article 126 de la LCE (via le présent article 2 de l'avant-projet de loi) applicable non seulement aux opérateurs, mais également aux fournisseurs et aux revendeurs. **Vu que ceux-ci n'étaient pas visés par la Directive 2006/24, ni par les implications pratiques mentionnées au point 11 et vu le passage précité de la justification de la loi du 20 juillet 2006 *portant des dispositions diverses*, la Commission estime recommandé de les soustraire à l'application de l'article 2 de l'avant-projet de loi et de les reprendre dans une autre disposition. En général, concernant les présents projets, il convient de faire remarquer que sous prétexte d'une transposition de la directive, on essaie d'imposer bien plus que ce que celle-ci prévoit, en tant que cadre maximum (comme par exemple viser également les réseaux privés en plus des réseaux publics, enregistrer des données supplémentaires, ...).**

21. La Commission fait en outre remarquer qu'un opérateur qui traite des données pour le compte de l'État, comme c'est le cas au point a) de l'article 2 de l'avant-projet de loi, agit en tant que son sous-traitant, tel que défini à l'article 1, § 5 de la LVP. L'État pourrait donc dans ce cas être considéré comme le responsable du traitement. Il faut dès lors recommander ici de préciser explicitement à l'article 2 que les opérateurs sont considérés comme des responsables du traitement au sens de la LVP.

22. L'Exposé des motifs et l'avant-projet de loi précisent que le nouvel article 126 s'applique sans préjudice des dispositions de la LVP. Dès lors, les opérateurs sont désormais explicitement tenus (ce qui était d'ailleurs déjà le cas auparavant) de respecter l'ensemble des dispositions de la LVP et de son arrêté d'exécution du 13 février 2001. Cela correspond aux dispositions de la directive qui prévoit également une application de la Directive 95/46/CE aux opérateurs[10].

23. L'Exposé des motifs stipule que les opérateurs et les fournisseurs doivent respecter la LVP, notamment en ce qui concerne les droits des personnes concernées : "*elle pourra accéder à ses données et pourra, le cas échéant, les faire rectifier ou supprimer*". Le droit de consultation, tel que prévu à l'article 10 de la LVP, et le droit de rectification (article 12) sont jugés d'application dans leur intégralité. Les fournisseurs ou les opérateurs devraient transmettre, sur demande, un aperçu complet des données conservées. À cet égard, il faut préciser que l'abonné d'un raccordement pourrait avoir, via le droit de consultation, une idée du comportement de communication ou des données de localisation de tous les utilisateurs sur une période plus longue. Dans ce contexte, on peut penser aux travailleurs ou aux membres de la famille, dont des mineurs. L'Exposé des motifs ignore, à tort, cette problématique. Dans le cadre de la téléphonie fixe et mobile, il existe des solutions pour protéger la vie privée, comme le masquage

[10] Voir les considérants 15 et 16.

des numéros. Toutefois, cela ne vaut pas pour Internet. En effet, pour la transmission d'e-mails, aucune facture spécifiée n'est fournie et il ne semble donc pas y avoir non plus de solution pour masquer les données d'adresse.

24. L'article 2 prévoit aux points a), b) et c) les finalités particulières pour lesquelles les données de trafic, de localisation et les données d'identification des utilisateurs peuvent être utilisées. À cet égard, on peut formuler les remarques suivantes :

25. La finalité prévue au point a) : *recherche, poursuite et répression d'infractions pénales* constitue une transposition de la Directive 2006/24, dont le but est la recherche, la détection et la poursuite d'**infractions graves**. L'avant-projet de loi ne fait toutefois référence qu'à des infractions pénales, ce qui implique *de facto* que les données conservées peuvent être utilisées pour n'importe quelle infraction pénale, y compris des contraventions. Ceci n'est certainement pas conforme au principe de la directive, ni au principe de proportionnalité, qui prévoient la conservation de certaines données pour la lutte contre le crime organisé et le terrorisme, et donc pas pour n'importe quel délit (cf. ci-dessus, points 4-6).

26. Par analogie avec par exemple la loi MPR[11] ou l'article 90*ter* du CIC concernant les écoutes de communications privées, le législateur pourrait prévoir dans l'actuel avant-projet de loi une énumération stricte des délits graves pour la recherche, la poursuite et la répression desquels les données conservées peuvent être utilisées. Il faut au moins tenir compte des articles 46*bis* et 88*bis* du CIC, qui prévoient actuellement respectivement la réclamation, par le procureur du Roi, de données d'identification relatives à un service de télécommunication et la réclamation, par le juge d'instruction, de données de localisation d'une télécommunication. De cette manière, il serait également plus clair de savoir qui a accès aux données conservées, pour les finalités mentionnées au point a). À ce sujet, les projets ne prévoient rien, à l'exception de l'accès interne au sein des opérateurs (Cellule de coordination de la Justice). La directive stipule à l'article 4, concernant l'accès aux données, que les États membres doivent prendre *les mesures nécessaires pour veiller à ce que les données conservées ne soient transmises qu'aux autorités nationales compétentes, dans des cas précis et conformément au droit interne*.

27. **En outre, tout autre usage de ces données devrait être punissable et une sanction de nullité devrait également y être liée.** Voir à cet égard ce qui est stipulé à l'article 13, point 2 de la directive : "*Chaque État membre prend, en particulier, les mesures nécessaires pour faire en sorte que l'accès intentionnel aux données conservées conformément à la présente directive ou le transfert de ces données qui ne sont pas autorisés par le droit interne adopté en*

[11] Loi du 6 janvier 2003 *concernant les méthodes particulières de recherche et quelques autres méthodes d'enquête.*

application de la présente directive soient passibles de sanctions, y compris de sanctions administratives ou pénales, qui sont efficaces, proportionnées et dissuasives." Étant donné que l'IBPT est compétent[12] pour contrôler le respect de la loi du 13 juin 2005 *relative aux communications électroniques* et des arrêtés d'exécution y afférents, la possibilité de sanctions alternatives est prévue, notamment des amendes administratives, que l'IBPT peut infliger en vertu de l'article 21 de la loi du 17 janvier 2003. Les projets ne stipulent toutefois pas explicitement quelle instance publique contrôle la sécurité des données conservées, ce qui est néanmoins prévu par l'article 9 de la directive. **Il convient de recommander de reprendre les autorités de contrôle dans l'avant-projet de loi, de même que leurs compétences et les sanctions, et de ne pas seulement y faire référence dans l'Exposé des motifs.**

28. Qu'en est-il de la preuve obtenue en dépit des dispositions de cette loi, par exemple par des personnes qui ne sont pas compétentes pour disposer de ces informations ? Si l'on souhaite exclure un tel moyen de preuve, il est recommandé de le prévoir explicitement dans l'avant-projet de loi, et **d'imposer la nullité d'une telle preuve**. La doctrine d'Antigone[13] de la Cour de cassation n'exclut en effet pas *ipso facto* la preuve obtenue de manière irrégulière.

29. Le point b) de l'article 2 de l'avant-projet de loi mentionne 'la répression d'appels malveillants vers les services d'urgence'. Le point c) prévoit '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'. Ces points ne découlent pas de la transposition de la Directive 2006/24 mais sont prévus dans des dispositions spécifiques. Conformément à l'article 43*bis*, § 3, 7° de la loi du 21 mars 1991[14], le Service de Médiation est chargé d'*examiner la demande de toute personne se prétendant victime d'une utilisation malveillante d'un réseau ou d'un service de communications électroniques visant à obtenir communication de l'identité et de l'adresse des utilisateurs de réseaux ou de services de communications électroniques l'ayant importunée, pour autant que ces données sont disponibles*.

---

[12] Voir l'article 14 de la loi du 17 janvier 2003 *relative au statut du régulateur des secteurs des postes et des télécommunications belges.*

[13] Voir notamment à cet égard l'arrêt de la Cour de cassation du 14 octobre 2003, T. Strafr. 2004, 129 avec note de Ph. TRAEST.

[14] Loi du 21 mars 1991 *portant réforme de certaines entreprises publiques économiques*.

30. **Les points b) et c) ne font pas partie de la transposition de la Directive 2006/24. Étant donné que les finalités de ces points n'ont aucun rapport avec des 'infractions graves', on peut se demander pour quelle raison les points a), b) et c) sont repris dans le même article et traités de la même façon dans l'avant-projet de loi et le projet d'arrêté royal.** En effet, aucune distinction n'est prévue quant aux données conservées auxquelles on peut recourir, ni quant à la durée d'utilisation de ces données. Pour le point b) par exemple, l'accès aux données relatives aux services de courriers électroniques ne semble pas être nécessaire. Il n'est pas non plus démontré pour quelle raison ces données devraient être accessibles pendant 24 mois pour cette finalité. **En raison du principe de proportionnalité et du principe de finalité, repris à l'article 4 de la LVP, l'avant-projet de loi ou du moins le projet d'arrêté royal devrait prévoir une distinction entre les points susmentionnés. Idéalement, les points b) et c) doivent être régis dans une législation distincte.**

31. L'article 2, § 1er de l'avant-projet de loi prévoit en outre ce qui suit : "*Le Roi fixe, par arrêté délibéré en Conseil des Ministres, sur proposition du Ministre de la Justice et du Ministre, et après avis de la Commission de la protection de la vie privée et de l'Institut, les données à conserver en application de l'alinéa 1er ainsi que les conditions et la durée de conservation de ces données.*"

32. **La Commission fait remarquer que le choix de ne pas reprendre les types de données dans le texte même de la loi mais dans un arrêté royal est difficilement compatible avec le choix formulé dans la Directive 2006/24 au sujet des données à conserver.** Initialement, la Commission européenne avait en effet proposé de joindre une liste de données en annexe à la directive, ce qui aurait permis une procédure accélérée du processus décisionnel pour des adaptations de cette liste. Le Parlement européen a toutefois adopté, à une large majorité, un amendement du rapporteur Alvaro visant à reprendre les données dans le texte même de la directive. On opte ainsi également pour une procédure plus lourde d'adaptation des types de données à conserver, avec un consentement complet dans le chef du Parlement européen. **Une même remarque doit être formulée en ce qui concerne le délai de conservation des données, cf. ci-dessous aux points 33 et suivants.** Ce qui précède vaut d'autant plus que dans l'Exposé des motifs, il est stipulé que le cadre pour la conservation des données, tel que prévu par la directive, ne répond pas nécessairement aux besoins des services de police et des autorités judiciaires. Cela explique pour quelle raison on souhaite reprendre dans le projet d'arrêté royal des données supplémentaires qui ne sont pas prévues par la directive, telles que des données bancaires.

33. Quant à la durée de conservation, l'article 2, § 1er de l'avant-projet de loi prévoit ce qui suit : "*La durée de la conservation des données visées à l'alinéa 1er ne peut être inférieure à 6 mois ni dépasser 24 mois.*" L'article 6 de la directive précise que les données peuvent être conservées pendant un minimum de 6 mois et un maximum de 24 mois, à compter de la date de la communication. En ce qui concerne la durée, le projet d'arrêté royal opte pour la durée maximale de 24 mois prévue par la directive. Le Rapport au Roi motive ce choix sommairement, en affirmant que "*la pratique observée auprès des différents services de police décentralisés ou auprès du Parquet fédéral en matière de demandes d'informations aux opérateurs et aux fournisseurs de réseaux ou de services de communications électroniques, amène à considérer qu'un délai uniforme de vingt-quatre mois pour la conservation des différents types de données visés à l'article 126 de la loi, constitue le mécanisme le plus approprié.*"[15]

34. La Directive 2006/24 prescrit à l'article 6 un délai de conservation de minimum 6 mois et de maximum 2 ans. Le Groupe 29 a toujours maintenu le point de vue selon lequel l'instauration d'une obligation de conservation pour les données de trafic historiques de tous les citoyens était une mesure très radicale dont la nécessité devait être prouvée de manière irréfutable[16]. L'article 8 de la CEDH consacre le droit fondamental des citoyens au respect de leur vie privée. Les autorités ne peuvent porter préjudice à ce droit par une loi que dans la mesure où cela est *nécessaire* dans une société démocratique. La nécessité impose de grandes exigences concernant la proportionnalité de chaque mesure spécifique qui limite la vie privée des citoyens. Les dispositions générales de la directive ne changent rien au fait que chaque mise en œuvre nationale doit être confrontée de manière indépendante à l'article 8 de la CEDH et à la jurisprudence y afférente de la Cour européenne des Droits de l'Homme. Cela vaut explicitement pour la nécessité d'un délai de conservation plus long que le délai nécessaire à la gestion d'entreprise des fournisseurs-opérateurs.

35. La Commission constate que le Rapport au Roi donne peu d'explications quant à la manière dont le délai maximum de 24 mois a été fixé. On fait référence à la pratique auprès des différents services

---

[15] Rapport au Roi, page 1.

[16] Voir l'avis 4/2001 *concernant le projet de convention du Conseil de l'Europe sur la cybercriminalité*, l'avis 10/2001 *sur la nécessité d'une approche équilibrée dans la lutte contre le terrorisme*, l'avis 4/2005 *sur la proposition de directive du Parlement européen et du Conseil sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, et modifiant la directive 2002/58/CE* et l'avis 3/2006 *sur la directive 2006/24/CE du Parlement européen et du Conseil 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 communication, et modifiant la directive 2002/58/CE*.

de police. La Commission demande que la nécessité de ce délai de conservation soit justifiée de manière plus précise et qu'elle soit étayée. À l'instar des récents avis du Groupe 29 sur ce sujet, la Commission recommande dès lors une application minimale harmonisée des dispositions de la directive, avec un délai de conservation qui diverge le moins possible de la finalité initiale pour laquelle les données sont enregistrées par les fournisseurs de services de communication. Il est nécessaire d'étayer par des arguments convaincants la durée d'une obligation de conservation qui est en effet contraire à l'obligation générale de destruction de la Directive 2002/58/CE. "*Comme indiqué ci-dessus, la justification d'une conservation systématique et obligatoire des données doit être clairement démontrée et étayée de preuves. Ce principe s'applique également aux périodes maximales à fixer*."[17]

36. De plus, la Commission fait remarquer que le principal fondement de la directive, formulé à l'article premier, est l'harmonisation des dispositions des États membres relatives aux obligations en matière de conservation, en vue de garantir la disponibilité des données à des fins de recherche, de détection et de poursuite d'infractions graves. Compte tenu des mises en œuvre et des propositions dans d'autres États membres de l'Union européenne dont la Commission a connaissance, elle constate que jusqu'à présent, il est peu question d'une quelconque harmonisation du délai de conservation. L'Allemagne semble opter pour un délai de conservation de 6 mois, tout comme la Finlande et la Tchéquie. La Suède, un des quatre pays à l'initiative de la réalisation d'une obligation de conservation au niveau européen, semble également opter pour une mise en œuvre minimale. D'autres pays comme la France, le Danemark et l'Espagne optent pour un délai de conservation de 12 mois. Les Pays-Bas semblent également opter pour un délai de 12 mois. Pour autant que l'on sache, seule l'Italie opte pour une durée de conservation de 24 mois, et ce uniquement pour les données téléphoniques, l'enregistrement des données Internet étant de 6 mois.

37. **Vu ce qui précède, la Commission estime que la durée de conservation de 24 mois actuellement prévue doit être davantage étayée par des arguments plus convaincants. En l'absence d'une telle justification, une adaptation du délai prévu doit être envisagée, le cas échéant, certainement compte tenu des délais de conservation en vigueur dans la plupart des autres pays européens, qui vont actuellement de 6 à 12 mois.**

38. L'article 2, § 2 de l'avant-projet de loi prévoit que "*si des circonstances particulières le justifient, le Roi peut, après avis de l'Institut et de la Commission de la protection de la vie privée, et ce pour une période limitée, fixer un délai de conservation des données supérieur à 24 mois.*"

[17] Avis 4/2005 du Groupe 29, page 8.

39. La Commission souligne tout d'abord que la version néerlandaise et la version française de l'avant-projet de loi diffèrent en ce qui concerne la période, qui est 'une période *limitée*' dans la version française et 'een *onbeperkte* periode' dans la version néerlandaise. Conformément à l'article 12 de la directive, cette prolongation doit être limitée dans le temps, et la version néerlandaise doit être adaptée en conséquence.

40. Le Roi a donc ainsi la possibilité de fixer un délai plus long que le délai légal maximal de 24 mois, *dans des circonstances particulières*. L'article 12 de la directive formule ceci comme suit : "*Un État membre confronté à des circonstances particulières justifiant une prolongation, pour une période limitée, de la durée de conservation maximale prévue à l'article 6, peut prendre les mesures nécessaires.*" S'il s'agit d'une exception, il est pour le moins nécessaire, aux yeux de la Commission, de régler le principe de base de cette exception de manière formelle dans la loi. Cette règle générale peut ensuite être développée ultérieurement dans un arrêté royal, mais le fondement devrait être ancré dans la loi, ce qui n'est pas le cas : **les termes 'circonstances particulières' n'offrent pas suffisamment de sécurité juridique, sont extrêmement vagues et sont dès lors sujets à une trop grande interprétation.**

D.5. ANALYSE DU PROJET D'ARRÊTÉ ROYAL

D.5.1. Examen général du projet d'arrêté royal

41. En ce qui concerne la durée de conservation de 24 mois qui est prévue dans le projet d'arrêté royal, la Commission renvoie aux remarques formulées aux points 33 et suivants. Elle rappelle également que la durée de conservation et les types de données conservées devraient de préférence être définis dans la loi et non dans le projet d'arrêté royal, cf. supra au point 32.

42. La durée de conservation est abordée différemment dans le projet d'arrêté royal selon la nature des données : les données servant à l'identification de l'abonné et du service utilisé sont conservées pendant toute la durée de l'abonnement et pour une période de 24 mois à compter du jour où l'abonnement expire. Les données de trafic et de localisation sont conservées pour une période de 24 mois à compter du jour où elles ont été générées ou traitées par le fournisseur de services. Ce qui précède semble aller à l'encontre du texte de la directive, où la durée de conservation débute à compter de la date de la communication.

43. L'Exposé des motifs[18] stipule que la directive prévoit un cadre minimum pour la conservation des données en matière de communication électronique, qui ne répond pas nécessairement aux besoins des services de police et des autorités judiciaires dans leurs missions de recherche, de poursuite et de répression d'infractions pénales. D'après l'Exposé des motifs, il manque ainsi, dans la liste établie par la directive, certaines données qui sont indispensables en vue de l'identification de personnes concernées par une communication pertinente dans le cadre d'une enquête en matière répressive, telles que des données bancaires. À noter que l'Exposé des motifs affirme que des données supplémentaires sont nécessaires pour l'enquête en matière répressive, mais que ces données sont également rendues publiques, ou du moins ne sont pas verrouillées, pour des enquêtes effectuées par le Service de médiation ou dans le cadre de la répression d'appels malveillants vers les services d'urgence. Comme déjà remarqué ci-dessus aux points 22 et 23, il faut préciser qui a accès à quelles données. À la lumière du principe de proportionnalité, on ne peut en effet avoir accès qu'aux données dont on a besoin réellement. Quoi qu'il en soit, la Commission ne peut pas adhérer à la considération de l'Exposé des motifs selon laquelle la directive prévoirait un cadre minimum : la directive prescrit de manière détaillée à l'article 5 quelles catégories de données doivent être conservées. Au considérant 21, la directive stipule que ses objectifs sont la recherche, la détection et la poursuite d'infractions graves et qu'elle n'excède pas ce qui est nécessaire pour atteindre ces objectifs. D'après le considérant 12 de la directive, la liste des "catégories de données" doit être comprise comme un cadre maximum. Pour la conservation d'autres données, les États membres peuvent recourir à l'article 15, premier alinéa de la Directive 2002/25/CE. **La législation qui est promulguée sur la base de cet article doit répondre de manière distincte à l'exigence de l'article 8 de la CEDH, à savoir qu'elle doit être, dans une société démocratique, nécessaire, raisonnable et proportionnelle en vue de garantir la sécurité nationale ou de prévenir, rechercher et poursuivre des infractions pénales.** La Commission a réclamé aux rédacteurs du projet une liste reprenant les données supplémentaires à conserver - c'est-à-dire en sus de ce qui est prévu dans la directive. Une telle liste n'a toutefois pas encore pu lui être fournie, de sorte que la Commission tente de vérifier elle-même ci-après – sous réserve d'une mauvaise interprétation – ce qui correspond à la directive et ce qui s'en écarte. La Commission a fait remarquer à cet égard que, pour chaque catégorie de données, l'on conserve visiblement davantage dans le projet d'arrêté royal que ce qui est prévu dans la directive, que ce choix soit motivé ou non. La Commission s'y penchera de plus près ci-dessous dans la discussion des articles.

[18] Exposé des motifs, p. 1-2.

D.5.2. Discussion des articles du projet d'arrêté royal

ARTICLE 1er

44. Cet article définit plusieurs notions, parmi lesquelles celle de "données personnelles" : on entend par là les nom et prénom et les adresses de facturation et de contact de l'abonné ou de l'utilisateur. Il y a lieu de préciser que cette définition ne correspond pas à celle des "données à caractère personnel" de l'article 1, § 1 de la LVP, qui est beaucoup plus large. La Commission part dès lors du principe que le but n'est pas d'utiliser ici la même définition que celle prévue par la LVP.

ARTICLE 2

45. L'article 2 concerne les données que doivent conserver les opérateurs en téléphonie fixe, c'est-à-dire ceux qui proposent un service de téléphonie fixe accessible au public. Ces données sont réparties en deux catégories : d'une part, les données relatives à l'identification de l'abonné ou à l'identification du service utilisé et, d'autre part, les données relatives au trafic et à la localisation lors d'une communication.

46. La première catégorie comprend principalement les données fournies par l'abonné lors de la souscription de son abonnement, ou au cours de celui-ci. **La Commission fait remarquer que seuls les éléments 1° et 2° (le numéro attribué à l'abonné et les données personnelles de l'abonné) sont prévus par l'article 5 de la directive, mais manifestement pas les éléments 3° à 8° inclus.** Cette extension n'est pas motivée, sauf par l'Exposé des motifs qui affirme que le cadre de la directive ne répond pas nécessairement aux besoins des services de police et des autorités judiciaires dans leurs missions de recherche, de poursuite et de répression d'infractions pénales. Concernant l'élément 6°, le commentaire des articles stipule que "*Ces données peuvent se révéler extrêmement importantes afin de déterminer vers quel opérateur les autorités judiciaires devront éventuellement se tourner pour obtenir des informations antérieures ou postérieures à une période donnée*." En ce qui concerne l'élément 7°, les données bancaires, la Commission remarque que ces données peuvent être obtenues auprès des banques par les enquêteurs, étant donné que ces derniers disposent des données d'identité. Dans quelle mesure est-il donc proportionnel de reprendre ces données ici ?

47. La collecte des éléments 3° à 8° inclus va au-delà de la liste prévue à l'article 5 de la directive. Comme déjà précisé ci-dessus, cette liste doit être considérée comme un cadre maximum en vertu du considérant 12 de la directive. Pour conserver d'autres données, les États membres peuvent recourir à l'article 15, premier alinéa de la Directive 2002/25/CE. La législation qui est promulguée sur la base de cet article doit répondre de manière distincte à l'exigence de l'article 8 de la CEDH, à savoir qu'elle doit être, dans une société démocratique, nécessaire, raisonnable et proportionnelle en vue de garantir la sécurité nationale ou de prévenir, rechercher et poursuivre des infractions pénales. Jusqu'à présent, le projet d'arrêté royal n'y satisfait pas.

48. La deuxième catégorie de données est constituée de données générées lors d'une communication. La Commission n'a pas de remarque à formuler à cet égard.

ARTICLE 3

49. Cet article concerne les données que doivent conserver les opérateurs en téléphonie mobile, c'est-à-dire ceux qui proposent un service de téléphonie mobile accessible au public. Ces données sont réparties en deux catégories : d'une part, les données relatives à l'identification de l'abonné ou à l'identification du service utilisé et, d'autre part, les données relatives au trafic et à la localisation lors d'une communication.

50. La première catégorie comprend principalement les données fournies par l'abonné lors de la souscription de son abonnement, ou au cours de celui-ci. **La Commission fait remarquer que seuls les éléments 1° et 2° (le numéro attribué à l'abonné et les données personnelles de l'abonné) sont prévus par l'article 5 de la directive, mais manifestement pas les éléments 3° à 10° inclus.** Cette extension est motivée sommairement, principalement par l'Exposé des motifs qui affirme que le cadre de la directive ne répond pas nécessairement aux besoins des services de police et des autorités judiciaires dans leurs missions de recherche, de poursuite et de répression d'infractions pénales. Concernant les éléments 3° et 4°, le commentaire des articles stipule que *"Savoir quand la carte a été achetée, et quand elle a été utilisée la première fois peut fournir des indices précieux aux enquêteurs.* (...) *La conservation des informations relatives à la recharge de crédit liée à une carte prépayée permet de connaître la capacité d'utilisation dont dispose l'utilisateur, le mode de recharge qu'il a utilisé, ou encore l'endroit où la recharge a été effectuée. Ce type d'information sort du cadre des données normalement visées par la directive mais représente un réel intérêt dans le cadre d'une enquête où ce peu d'information est souvent la seule piste dont disposent*

les services de police afin de tenter d'identifier un suspect." La Commission suit cette explication, mais estime, en raison des remarques déjà formulées aux points 43 et 47, que cela ne suffit pas pour aller au-delà de ce qui est prévu par la directive.

51. La deuxième catégorie de données est constituée de données générées lors d'une communication. La Commission n'a pas de remarque à formuler à cet égard.

ARTICLE 4

52. Cet article vise les fournisseurs d'un accès à l'Internet. Ces données sont réparties en deux catégories : d'une part, les données relatives à l'identification de l'abonné ou à l'identification du service utilisé et, d'autre part, les données relatives au trafic et à la localisation.

53. La première catégorie comprend principalement les données fournies par l'abonné lors de la souscription de son abonnement, ou au cours de celui-ci. **La Commission fait remarquer que seuls les éléments 1° et 2° (le code identifiant attribué à l'abonné et les données personnelles de l'abonné) sont prévus par l'article 5 de la directive, mais manifestement pas les éléments 3° à 8° inclus.** Cette extension est motivée sommairement par l'Exposé des motifs qui affirme que le cadre de la directive ne répond pas nécessairement aux besoins des services de police et des autorités judiciaires dans leurs missions de recherche, de poursuite et de répression d'infractions pénales. La Commission prend note de cette explication mais estime, en raison des remarques déjà formulées aux points 43 et 47, que cela ne suffit pas pour aller au-delà de ce qui est prévu par la directive.

54. La deuxième catégorie de données comprend des données relatives au trafic et à la localisation. **La Commission fait remarquer que seuls les éléments 1° à 4° inclus et 6° (mais d'après la directive, uniquement pour le début, pas pour la fin) sont prévus par l'article 5 de la directive, mais manifestement pas les éléments 5° et 7°.** Cette extension n'est pas motivée, et ne peut dès lors pas être suivie vu les remarques déjà formulées ci-dessus.

ARTICLE 5

55. L'article 5 vise les données à conserver par les fournisseurs de services de courriers électroniques et par les fournisseurs de services téléphoniques par Internet. Par fournisseurs de services de courriers électroniques, on vise tant les courriers SMTP que les webmails tels que Hotmail, Yahoo, Gmail, ... Ces données sont réparties en deux catégories : d'une part, les données relatives à l'identification de l'abonné ou à l'identification du service utilisé et, d'autre part, les données relatives au trafic et à la localisation.

56. En ce qui concerne les services de webmail tels que Hotmail et Gmail, on ne sait pas clairement sur quelle base ils sont soumis à l'obligation de conservation. Ni l'Exposé des motifs, ni le Rapport au Roi n'apportent des précisions à cet égard.

57. La première catégorie comprend principalement les données fournies par l'abonné lors de la souscription de son abonnement, ou au cours de celui-ci, ou lorsqu'il utilise les services proposés. **La Commission fait remarquer que seuls les éléments 1° et 2° (le code identifiant de l'abonné ou de l'utilisateur et les données personnelles de l'abonné ou de l'utilisateur) sont prévus par l'article 5 de la directive, mais manifestement pas les éléments 3° à 6° inclus.** Cette extension est motivée sommairement par l'Exposé des motifs qui affirme que le cadre de la directive ne répond pas nécessairement aux besoins des services de police et des autorités judiciaires dans leurs missions de recherche, de poursuite et de répression d'infractions pénales. La Commission prend note de cette explication mais estime, en raison des remarques déjà formulées aux points 43 et 47, que cela ne suffit pas pour aller au-delà de ce qui est prévu par la directive.

58. La deuxième catégorie de données est constituée de données générées lors d'une communication. La Commission n'a pas de remarque à formuler à cet égard, sauf au sujet du point 7° (concernant ce point, la directive prévoit uniquement l'enregistrement de la localisation au début).

ARTICLE 6

59. Le premier alinéa de l'article 6 vise les opérateurs qui fournissent différents services combinés, tel que par exemple l'envoi de mails via un gsm. Les données qu'ils devront conserver dans le cas précité doivent correspondre à ce qui a été prévu tant à l'article 3 (téléphonie mobile) qu'à l'article 5 (courrier électronique) du projet d'arrêté royal. **La Commission se réfère aux remarques formulées ci-avant pour les articles 2 à 5 inclus, qui s'appliquent *mutatis mutandis* à l'article 6.**

60. Les deuxième et troisième alinéas concernent des dispositions relatives aux indications de l'heure, qui ont été reprises de l'arrêté royal du 9 janvier 2003. La Commission n'a pas de remarque à formuler à cet égard.

ARTICLE 7

61. D'après le commentaire des articles, l'article 7 fixe un certain nombre de conditions de conservation destinées à garantir la sécurité des données et à assurer leur traitement adéquat par du personnel autorisé. Les éléments 1°, 2° et 4° ont été directement repris de l'article 7 de la Directive 2006/24. Le point 1 prévoit un enregistrement distinct pour les données à conserver, ce qui concorde avec les recommandations du Groupe 29 qui prévoient un enregistrement décentralisé et tenu logiquement de manière distincte des données à conserver spécifiquement à des fins de recherche. D'un point de vue de la vie privée, il doit y avoir une distinction claire entre les données conservées par les opérateurs à des fins professionnelles et celles conservées dans le cadre des présents projets. Le projet d'arrêté royal reste par ailleurs relativement vague pour l'élément 2°, en ne faisant référence qu'à des "mesures techniques et organisationnelles appropriées", sans les développer davantage. À cet égard, la Commission se réfère pour information aux mesures de référence qu'elle a établies, lesquelles, selon le cas, doivent s'appliquer à un traitement de données à caractère personnel[19].

62. L'élément 3° oblige l'opérateur à garantir que seule la Cellule de coordination de la Justice visée à l'article 2 de l'arrêté royal du 9 janvier 2003 ait accès aux données.

[19] Voir à cet égard le document intitulé "Mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel" de la Commission de la protection de la vie privée, disponible sur son site Internet à l'adresse http://www.privacycommission.be/fr/static/pdf/mesures-de-r-f-rence-vs-01.pdf.

63. **La Commission fait tout d'abord remarquer à cet égard que seul l'accès aux données auprès des opérateurs eux-mêmes est ainsi régi, c'est-à-dire en interne, et non à qui ces données peuvent être transmises en externe.** Conformément à l'article 2, § 1 de l'arrêté royal précité : "*Pour satisfaire à l'obligation de collaboration imposée par les articles 46bis, § 2, 88bis, § 2 et 90quater, § 2, du Code d'Instruction criminelle, chaque opérateur d'un réseau de communications et chaque fournisseur d'un service de télécommunications désigne nommément une ou plusieurs personnes chargées d'assumer les tâches résultant de l'obligation de coopérer et dénommée(s) ci-après la 'Cellule de coordination de la Justice'*". Comme déjà indiqué aux points 26, 29 et 30, il faudrait prévoir clairement à qui quelles données peuvent être transmises par la Cellule de coordination de la Justice. Conformément à l'article 2, § 1, c) de l'avant-projet de loi, le Service de médiation pour les télécommunications devrait par exemple également pouvoir obtenir un droit de regard, ce qui n'est pas prévu explicitement au stade actuel. **Il convient de déterminer clairement et de manière limitative, de préférence dans l'avant-projet de loi, qui a accès aux données conservées, à quelles données en particulier et pour quelles finalités spécifiques.**

64. **Il convient en outre de répéter que cette cellule de coordination n'a été installée par l'arrêté royal du 9 janvier 2003 qu'auprès des opérateurs et non auprès des fournisseurs et revendeurs mentionnés à l'article 9, §§ 5 et 6 de la LCE.** Le but est-il que les fournisseurs et revendeurs créent également une telle cellule de coordination, qui doit répondre aux mêmes dispositions, notamment en matière de disponibilité 24h/24 et 7j/7 ? Comme déjà remarqué ci-avant au point 16, le législateur a exclu précédemment cette égalité de traitement entre les opérateurs d'une part et les fournisseurs et revendeurs d'autre part, en n'y faisant pas référence dans la version actuelle de l'article 126 de la LCE, mais bien à l'article 9, § 7 de cette même loi, qui prévoit un règlement distinct pour cette catégorie.

65. **Ensuite, "la garantie" de l'opérateur que seule la Cellule de coordination de la Justice ait accès n'est pas suffisante ; le non-respect de cette règle d'accès interne devrait être sanctionné pénalement.** Voir à ce sujet ce qu'énonce l'article 13, point 2 de la directive : "*Chaque État membre prend, en particulier, les mesures nécessaires pour faire en sorte que l'accès intentionnel aux données conservées conformément à la présente directive ou le transfert de ces données qui ne sont pas autorisés par le droit interne adopté en application de la présente directive soient passibles de sanctions, y compris de sanctions administratives ou pénales, qui sont efficaces, proportionnées et dissuasives.*"

66. Enfin, chaque opérateur doit veiller à ce que les données soient détruites à l'expiration du délai de conservation, à l'exception des données auxquelles on a pu accéder et qui ont été

préservées. Aucun délai de conservation n'est prévu à l'égard de ces dernières données. Il semblerait toutefois logique que si les données ont été consultées dans le cadre d'une enquête judiciaire, celles-ci soient conservées ultérieurement par les services responsables pour la durée nécessaire à leur enquête et puissent être détruites chez l'opérateur. Si les instances qui mènent l'enquête estimaient toutefois que les données ne sont pas utiles pour l'enquête, il n'est pas nécessaire de faire conserver les données par l'opérateur au-delà du délai de conservation prévu.

ARTICLES 8 ET 9

67. La Commission n'a pas de remarque à formuler à cet égard.

ARTICLE 10

68. Cet article dispose que le projet d'arrêté royal s'applique également aux tentatives d'appel ayant échoué. La Directive 2006/24 dispose à l'article 3, point 2 qu'elle n'impose pas la conservation des données relatives aux appels non connectés, mais bien concernant les appels téléphoniques infructueux, ce qui constitue, selon la directive, toute communication au cours de laquelle un appel téléphonique a été transmis mais est resté sans réponse ou a fait l'objet d'une intervention de la part du gestionnaire du réseau[20].

69. La formulation de l'article 10 ne correspond pas tout à fait, affirmant que l'arrêté s'applique également aux appels qui n'ont pas pu aboutir en raison d'une intervention de la part du gestionnaire de réseau. Il serait recommandé de reformuler ce passage, par exemple comme suit : " (...) *également aux appels qui ont fait l'objet d'une intervention de la part du gestionnaire du réseau*."

ARTICLE 11

70. D'après le commentaire des articles, l'article 11 institue, au sein de chaque Cellule de coordination de la Justice, un préposé à la protection des données, comme le permet l'article 17*bis*, alinéas 2 et 3 de la LVP. L'article 11, alinéa 3 vise à garantir l'indépendance du préposé dans ses fonctions.

[20] Voir l'article 2, f) de la Directive 2006/24/CE.

71. La Commission souligne que le Roi n'a pas encore fixé le statut des préposés à la protection des données en application de l'article 17*bis* de la loi LVP. Il serait donc prématuré d'anticiper des dispositions futures. Toutes les définitions de fonctions de contrôle, qu'elles soient internes ou non, devraient donc tenir compte de la Directive 95/46/CE (considérant (49) et article 18). Les préposés à la protection des données visés ici devraient en pratique être des interlocuteurs privilégiés de la Commission, ce qui est encouragé dans le projet d'arrêté royal par l'obligation de communiquer à la Commission leurs données d'identification et leurs coordonnées. Il est également recommandé que le projet d'arrêté royal assure une grande visibilité pour leurs avis et rapports. Dans cette optique, la Commission recommande que le projet d'arrêté royal soit adapté de manière à ce que ces rapports lui soient également communiqués de manière systématique.

72. L'indépendance des préposés à la protection des données est primordiale. Il importe toutefois qu'elle soit garantie par des mesures appropriées. Les mesures suivantes peuvent être intégrées dans le projet d'arrêté royal, outre celles déjà mentionnées à l'article 11 :

• communication à la Commission de la nature du lien juridique entre ces préposés et le service dans lequel ils exerceront leur fonction de préposé, de tous les éléments concernant les qualifications professionnelles relatives à la fonction de préposé, des mesures prises par le responsable du traitement en fonction des missions que doit exercer le préposé à la protection des données ;

• obligation de placer les préposés à un niveau de la hiérarchie tel qu'ils aient la possibilité de communiquer directement avec le management/comité de direction et d'exercer leur mission directement auprès du responsable du traitement.

73. Il convient enfin de répéter que l'article 11, § 2, 3° doit être précisé, cf. le point 63 ci-dessus, étant donné que ni le projet d'arrêté royal, ni l'avant-projet de loi n'établissent clairement qui, au sein de la Cellule de coordination de la Justice, a accès en externe aux données conservées.

ARTICLE 12

74. L'article 12 oblige les opérateurs concernés à communiquer annuellement à l'Institut un certain nombre d'informations statistiques qui seront destinées à la Commission des Communautés européennes. Étrangement, l'article 12 n'impose cela qu'à "l'opérateur fournissant un service de téléphonie accessible au public". Si l'on choisit de déclarer que l'avant-projet de loi et le projet d'arrêté royal s'appliquent également aux fournisseurs et revendeurs visés à l'article 9, §§ 5 et 6 de la LCE, ils doivent également être repris dans cet article. Il ne s'agit pas non plus, conformément à l'article 10 de la directive, d'un "service de téléphonie", mais bien d'un service de communication électronique ou d'un réseau de communication.

ARTICLES 13 ET 14

75. La Commission n'a pas de remarque à formuler à cet égard.

PAR CES MOTIFS,

la Commission estime que :

- vu le principe de légalité, les éléments essentiels en matière de conservation de données doivent être définis clairement dans l'avant-projet de loi. Dans cette optique, la durée de conservation devrait être définie dans l'avant-projet de loi, de même que les données à conserver ;
- la nécessité de conserver certaines données qui ne sont pas prévues dans la directive doit être justifiée, conformément aux principes de l'article 8 de la CEDH ;
- l'avant-projet de loi devrait préciser pour la recherche, la poursuite et la répression de quelles infractions pénales (graves) les données conservées peuvent être utilisées ;
- la durée de conservation de 24 mois doit être davantage fondée et justifiée et, le cas échéant, reconsidérée au vu des délais de conservation prévus dans la plupart des pays européens ;
- l'application de l'avant-projet de loi et du projet d'arrêté royal aux fournisseurs et aux revendeurs prévus à l'article 9, §§ 5 et 6 doit être réexaminée et doit éventuellement être prévue pour eux dans une autre disposition ;
- la conservation des données pour les finalités prévues à l'article 2, § 1, b) et c) (les appels malveillants vers les services d'urgence et le Service de médiation pour les

télécommunications) doit être retirée de l'application de l'avant-projet de loi, et qu'il faut prévoir à cet égard une réglementation distincte ;

- des exceptions ne peuvent pas être régies par un arrêté royal, mais que le principe de base de l'exception doit au moins être réglé dans la loi. La notion de "circonstances particulières" de l'article 2, § 2 de l'avant-projet de loi est trop vague ;
- la désignation des personnes ou instances qui ont accès aux données conservées via la Cellule de coordination de la Justice doit être faite explicitement dans l'avant-projet de loi, en mentionnant également qui a accès à quelles données ;
- le non-respect des exigences en matière d'accès et d'utilisation des données collectées doit être sanctionné ;
- les autorités de contrôle doivent être explicitement désignées dans l'avant-projet de loi, de même que leurs compétences et les sanctions en la matière.

Vu les remarques formulées dans le présent avis, la Commission de la protection de la vie privée émet un avis *défavorable* quant au contenu actuel de l'avant-projet de loi et du projet d'arrêté royal.

Pour l'Administrateur e.c.,
Le Chef de section OMR,

(sé) Patrick Van Wouwe

Le Président,

(sé) Willem Debeuckelaere