Arrêté royal portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques

Meta-données

Source en ligne.

Table des matières

Texte

Rapport au Roi

Sire,

La Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications électroniques et modifiant la Directive 2002/58/CE (ci-après « la directive ») a été publiée au Journal officiel de l'Union européenne du 13 avril 2006.

Cette directive vise principalement à réduire les disparités législatives et techniques existant au sein des différents États membres de l'Union en ce qui concerne les dispositions relatives à la conservation de données en vue de la recherche, de la détection et de la poursuite d'infractions pénales graves.

Cette directive est partiellement transposée par :

- l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques (ci-après « la LCE ») ;
- l'arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demande judiciaires concernant les communications électroniques.

Le présent arrêté complète et achève la transposition en portant exécution de l'article 126.

L'article 126, § 2, alinéa 1er, de la LCE prévoit cette conservation en vue de la recherche, de la détection et de la poursuite d'infractions pénales visées aux articles 46bis et 88bis du Code d'instruction criminelle, en vue de la répression d'appels malveillants vers les services d'urgence, 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 et en vue de l'accomplissement des missions de renseignement en ayant recours aux méthodes de collectes de données visées aux articles 18/7 et 18/8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

L'article 126 de la LCE habilite le Roi à fixer :

- les données à conserver (voir paragraphes 1er et 2 des articles 3 à 6) ;
- les données qui sont soumises à l'article 126, § 3, alinéa 1er, et celles qui sont soumises à l'alinéa 2 du même paragraphe (voir paragraphe 3 des articles 3 à 6) ;
- les exigences auxquelles ces données doivent répondre (article 7) ;
- les mesures techniques et administratives que les fournisseurs de réseaux et services concernés doivent prendre en vue garantir la protection des données à caractère personnelle (article 8) ;
- les statistiques que ces fournisseurs transmettent à l'Institut belge des services postaux et des télécommunications (ci-après « IBPT ») et celles que l'IBPT transmet au ministre et au ministre de la Justice (article 9).

L'article 5 de la directive établit la liste minimale des données à conserver en les regroupant par

catégories selon qu'il s'agit de données nécessaires pour : a) retrouver et identifier la source d'une communication, b) identifier la destination d'une communication, c) déterminer la date, l'heure et la durée d'une communication, d) déterminer le type de communication, e) identifier le matériel de communication utilisé et f) localiser le matériel de communication mobile.

L'article 5.1. de la directive prévoit des sous-catégories au sein de chacune de ces catégories sur la base du type de service de communications électroniques visé. Les sous-catégories visent ainsi la téléphonie fixe en réseau, la téléphonie mobile, l'accès à l'internet, le courrier électronique par Internet et la téléphonie par Internet.

Le présent arrêté présente les données à conserver autrement que dans l'article 5 de la directive. En effet, il fait d'abord une distinction par type de services et réseaux publics de communications électroniques. Ainsi, l'arrêté distingue :

- les fournisseurs au public de services de téléphonie fixe, à l'exception de la téléphonie par internet accessible au public, et les fournisseurs de réseaux publics de communications électroniques sous-jacents (article 3) ;
- les fournisseurs au public de services de téléphonie mobile, à l'exception de la téléphonie par internet accessible au public, et les fournisseurs de réseaux publics de communications électroniques sous-jacents (article 4) ;
- les fournisseurs au public de services d'accès à l'internet, à l'exception du courrier électronique par internet accessible au public et de la téléphonie par l'internet accessible au public, et les fournisseurs de réseaux publics de communications électroniques sous-jacents (article 5) ;
- les fournisseurs au public de services de courrier électronique par internet et de téléphonie par l'internet accessibles au public, à l'exception de l'accès à l'internet accessible au public, et les fournisseurs de réseaux publics de communications électroniques sous-jacents (article 6).

Deux sous-catégories sont prévues selon le type de données à conserver pour chacune des catégories de fournisseurs susvisées.

Il s'agit d'une part des données qui sont liées à l'abonnement, à l'inscription au service ou à l'utilisation du service et qui permettent d'identifier l'utilisateur final, le service de communications utilisé et l'équipement terminal qui est présumé avoir été utilisé (ci-après la première catégorie de données). Ces données sont visées au paragraphe 1er des articles 3, 4, 5 et 6 de l'arrêté. Comme ces données ne varient pas ou peu, elles sont relativement « statiques ».

Il s'agit d'autre part des données de trafic et de localisation au sens des articles 2, 6° (données de trafic) et 2, 7° (données de la localisation) de la LCE (ci-après la seconde catégorie de données). Ces données sont visées au paragraphe 2 des articles 3, 4, 5 et 6 de l'arrêté. Ces données fluctuent constamment selon les communications et ont donc une nature « dynamique ».

L'article 1.2 de la directive prévoit d'ailleurs « qu'elle s'applique aux données relatives au trafic et aux données de localisation concernant tant les entités juridiques que les personnes physiques, ainsi qu'aux données connexes nécessaires pour identifier l'abonné ou l'utilisateur enregistré ». Le présent arrêté vise les données de localisation et de trafic (§ 2 des articles 3 à 6) ainsi que les données d'identification des utilisateurs finals, du service de communications électroniques utilisé et de l'équipement terminal qui est présumé avoir été utilisé (§ 1er des articles 3 à 6). Le but ultime de l'identification de l'équipement terminal qui est présumé avoir été utilisé et du service de

communications électroniques utilisé est de pouvoir identifier les utilisateurs finals participant à la communication électronique.

Les données devraient être conservées de manière à éviter qu'elles ne soient conservées plus d'une fois. Le fournisseur de réseau ou de service concerné se chargera de conserver, pour chaque communication, le numéro ou l'identifiant attribué à l'utilisateur final afin de pouvoir mettre en relation les données de trafic et de localisation avec les données d'identification.

Par ailleurs, le présent arrêté dépasse quelque peu le cadre minimum fixé par la directive pour les raisons suivantes.

Il s'agit d'abord de combler un certain nombre de lacunes dans le cadre européen. La directive européenne a en effet été élaborée rapidement, de sorte que certaines questions n'ont pas été prises en considération.

Ensuite, le cadre européen ne répond pas nécessairement aux besoins des services de police et des autorités judiciaires dans leurs missions de prévention, de recherche, de détection et de poursuite d'infractions pénales. Ainsi, le présent arrêté vise par exemple certaines données indispensables en vue de l'identification des personnes concernées par une communication pertinente dans le cadre d'une enquête en matière répressive - telles que les données relatives au paiement - qui ne figurent pas à la liste établie par la directive.

Il faut enfin souligner que la directive a été adoptée le 15 mars 2006. Entretemps, des évolutions technologiques et économiques ont eu lieu et ont été prises en compte dans le présent arrêté. On pense à cet égard en particulier à la conservation des ports source suite au partage d'une adresse IP entre plusieurs utilisateurs finals.

Si le présent arrêté ne complétait pas la liste de la directive par un nombre limité de données supplémentaires, l'efficacité de la rétention de données s'en trouverait diminuée.

La directive a été prise sur base de l'article 95 (et non 94) du Traité instituant la Communauté européenne (actuellement l'article 114 du Traité sur le fonctionnement de l'Union européenne), ce qui permet d'aller plus loin que ce que prévoit la directive. Par ailleurs, 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 communications électroniques (ci-après « directive vie privée et communications électroniques ») 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 cet article. A cet égard, le considérant 12 de la directive prévoit que « l'article 15, paragraphe 1er, de la Directive 2002/58/CE continue à s'appliquer aux données, y compris à celles relatives aux appels téléphoniques infructueux, dont la conservation n'est pas expressément requise par la présente directive et qui ne relèvent donc pas de son champ d'application, ainsi qu'à la conservation de données à d'autres fins que celles prévues par la présente directive, notamment à des fins judiciaires. » Le présent arrêté royal s’appuie sur l'article 15.1 de la directive « vie privée et communications électroniques » pour ce qui concerne les données non prévues dans la directive.

Les données demandées en plus de celles figurant sur la liste de la directive portent principalement sur l'identification des parties concernées, en particulier sur la source de la communication. L'objectif de l'identification par une autorité compétente est de retrouver le véritable utilisateur final d'un service de communication. Cette identification implique évidemment la nécessité de conserver

les données personnelles de l'utilisateur final. Toutefois, l'utilisation fréquente de fausses données d'identité impose également de recourir à d'autres données administratives et techniques disponibles chez les opérateurs :

- les différentes adresses disponibles ;
- les données techniques de la connexion utilisées pour s'enregistrer ;
- les données relatives au paiement du service de communications électroniques.

Ces données supplémentaires mettent les autorités non seulement sur la piste de l'utilisateur final effectif mais elles leur permettent également d'exclure que les victimes d'une fraude à l'identité soient impliquées à tort en tant qu'auteur dans un dossier judiciaire qui ne les concerne en rien. Les données supplémentaires préviennent également la violation ultérieure de la vie privée de ces personnes innocentes par des mesures d'enquête subséquentes plus intrusives, telles que l'interception de leurs communications ou une perquisition.

La quantité des données supplémentaires demandées est limitée car elles concernent principalement l'utilisateur final et non les données de trafic. La conservation de ces données est toutefois nécessaire pour permettre une utilisation judicieuse des données de trafic conservées. Les données dont la conservation est demandée sont pour la plupart déjà conservées par les opérateurs comme données client.

La police et la justice s'en servent déjà et ont pu dans plusieurs cas dépister des criminels qui, dans le cadre de la criminalité organisée, faisaient usage de connexions mobiles ou Internet apparemment anonymes.

Certaines données supplémentaires concernant l'abonnement au service de communications électroniques considéré doivent fournir aux autorités des indices complémentaires quant à l'utilité d'une demande d'information auprès d'un opérateur : les services supplémentaires auquel l'utilisateur final est abonné, le commencement et la fin de l'abonnement, l'opérateur précédent en cas de portabilité du numéro.

Ces données sont également limitées en nombre et sont, elles aussi, déjà conservées chez les opérateurs.

Par ailleurs, le considérant 23 de la directive prévoit qu' « étant donné que les obligations incombant aux fournisseurs de services de communications électroniques devraient être proportionnées, la présente directive leur prescrit de ne conserver que les données qui sont générées ou traitées lors de la fourniture de services de communication. Dans les cas où ces données ne sont pas générées ou traitées par ces fournisseurs, il n'y a pas d'obligation de les conserver. ». De la même manière, les fournisseurs de réseaux de communications électroniques publics ne sont tenus de conserver les données que dans la mesure où ils les génèrent ou les traitent. Ce principe est rappelé à l'article 126, § 1er, alinéa 1er, de la loi du 13 juin 2005, tel que modifié par la loi du 30 juillet 2013, qui impose à certains fournisseurs de conserver uniquement certaines données qui sont générées ou traitées par eux dans le cadre de la fourniture des services de communications électroniques. Par conséquent, les données à conserver en vertu des articles 3 à 6 du présent arrêté ne doivent être conservées par un fournisseur de réseau ou de service que s'il traite ou génère cette donnée.

À titre d'illustration : le présent arrêté royal prévoit la conservation par les fournisseurs non seulement des données concernant leurs abonnés mais également des données concernant le destinataire de la communication (voir article 3, § 2, 2°, pour la téléphonie fixe, l'article 4, § 2, 4°,

pour la téléphonie mobile et l'article 6, § 2, 3°, b, pour l'e-mail). A part le numéro de téléphone ou l'adresse électronique que l'auteur de la communication a utilisé pour atteindre le destinataire de la communication, un fournisseur d'un abonné (ci-après le fournisseur A) ne connaît pas les données concernant le destinataire de la communication lorsque ce dernier est l'abonné d'un autre fournisseur (ci-après le fournisseur B). Dès lors qu'il ne connaît pas ces données, il ne les traite pas ni ne les génère. Par conséquent, il ne doit pas les conserver. Par contre, comme le fournisseur A connaît tout de même le numéro de téléphone et l'adresse électronique susmentionné et les traite, il devra les conserver. Par ailleurs, il reviendra au fournisseur B de conserver les données relatives au destinataire de la communication ainsi que le numéro de téléphone de l'appelant ou l'adresse électronique de l'auteur de la communication. Ces différentes données (numéros de téléphone de l'appelant et de l'appelé et adresses électroniques de l'auteur et du destinataire de la communication) permettent aux autorités d'établir le lien entre les participants à la communication.

Lorsqu'une donnée n'est pas disponible ou n'existe pas, il n'y a pas d'obligation de la conserver, dès que le fournisseur ne la traite pas ni ne la génère. Ainsi, à titre d'illustration, l'article 5, § 2, 6°, du présent arrêté oblige les fournisseurs à conserver « 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. » Si ces données n'existent pas ou ne sont pas disponibles, les fournisseurs ne doivent pas les conserver. Si c'est le fournisseur du service concerné qui traite ou génère une donnée mais non le fournisseur du réseau sous-jacent, ce dernier fournisseur ne sera pas tenu de conserver la donnée en question.

L'avis 53.841/2/V du 26 août 2013 du Conseil d'État a été globalement suivi. La prise en compte de cet avis appelle les explications suivantes :

1) Le Conseil d'Etat estime qu'il ne ressort pas du dossier qui lui a été transmis que l'examen préalable de la nécessité de procéder à une évaluation d'incidence au sens de l'article 19/1 de la loi du 5 mai 1997 relative à la coordination de la politique fédérale de développement durable (dit test « EIDD ») a bien été réalisé.

L'article 2, 3°, de l'arrêté royal du 20 septembre 2012 portant exécution de l'article 19/1, § 1er, deuxième alinéa, du chapitre V/1 de la loi du 5 mai 1997 précitée dispense d'un examen préalable « la réglementation envisagée portant transposition d'une directive de l'Union européenne qui a fait l'objet d'une analyse d'impact similaire à une évaluation d'incidence, visée à l'article 2, 9°, de la loi ». C'est le cas pour le présent arrêté royal, dès lors que le texte de la directive avait été soumis à une évaluation de qualité sur les impacts sur le développement durable (avis du 19 janvier 2006 du Comité économique et social européen).

2) Selon le Conseil d'État, les articles 4, § 3, 5, § 3, 6, § 3, et 7, § 3, (actuellement les articles 3, § 3, 4, § 3, 5, § 3 et 6, § 3) paraphrasent l'article 126, § 3, alinéas 1er et 2 et doivent donc être omis. Les articles 4, § 3, 5, § 3, 6, § 3, et 7, § 3, actuellement les articles 3, § 3, 4, § 3, 5, § 3 et 6, § 3) ont été modifiés pour ne plus paraphraser l'article 126, § 3, alinéas 1er et 2 de la LCE. Cependant ces articles ne peuvent pas être simplement omis. En effet, l'article 126, § 3, alinéa 3, de la LCE prévoit : « 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 qui sont soumises à l'alinéa 1er et celles qui le sont à l'alinéa 2. ».

3) Selon le Conseil d'État, l'article 126 de la LCE se réfère à l'identification des utilisateurs finals alors que le projet d'arrêté royal se réfère à l'identification des abonnés et des utilisateurs.
La notion d'utilisateur dans le projet d'arrêté royal doit en effet être remplacée par la notion

d'utilisateur final, qui est également visée par l'article 126 de la LCE. Il est vrai que la directive se réfère à la définition d'utilisateur, mais elle contient sa propre définition d'utilisateur, qui est la suivante : « toute entité juridique ou personne physique qui utilise un service de communications électroniques accessible au public à des fins privées ou professionnelles sans être nécessairement abonnée à ce service » (article 2, b). Or cette définition est plus proche de la définition d'utilisateur final au sens de la LCE (article 2, 13°) que de la définition d'utilisateur au sens de cette même loi (article 2, 12°).

Il n'est pas nécessaire de viser l'utilisateur enregistré comme le mentionne à certains endroits la directive. En effet, un fournisseur ne devra conserver des données que s'il les traite ou les génère (cf. supra). Par conséquent, si un fournisseur ne dispose pas d'une donnée d'un utilisateur final, car ce dernier n'est pas enregistré, il ne doit pas conserver cette donnée.
Il n'est pas nécessaire non plus de mentionner l'utilisateur final et l'abonné car la notion d'utilisateur final (article 2, 13°, de la LCE) inclut la notion d'abonné (article 2, 15°, de la LCE).

4) Selon le Conseil d'État, il faut reprendre la définition de « numéro d'identifiant » inscrite à l'article 2, d), de la directive.

C'est la définition en néerlandais « gebruikersidentificatie » de la directive qui a été préférée à la définition en français « numéro d'identifiant », car la définition en français semble constituer une mauvaise traduction par rapport aux autres versions linguistiques de la directive. Par ailleurs, comme indiqué ci-dessus, en droit belge, la notion « d'identifiant d'un utilisateur » utilisée par la directive doit être transposée par la notion d' « identifiant d'un utilisateur final ».

Commentaire des articles

Article 1er

Cet article ne nécessite pas de commentaire.

Article 2

L'article deux définit quelques notions en vue de l'application du présent arrêté.
Les définitions d'identifiant d'un utilisateur final et d'identifiant cellulaire constituent une transposition de concepts définis dans l'article 2 de la directive.

L'identifiant cellulaire est défini comme « le numéro d'identification de la cellule où un appel de téléphonie mobile a commencé ou a pris fin ». Une cellule dans un réseau mobile est un secteur géographique dont la couverture radio est fournie par une station de base du réseau. Chaque cellule a une identification unique dans le réseau, appelée « Cell-ID » ou identifiant cellulaire, qui fait en sorte que chaque utilisateur final puisse être clairement localisé dans le réseau afin de router un appel vers la bonne antenne et d'ainsi établir la connexion entre l'appelant et l'appelé.

Alors que la directive vise les noms et adresse de l'abonné ou de l'utilisateur inscrit (voir article 5.1, a), 1), ii), article 5.1, a), 2), iii), article 5.1., b), 1), ii) et article 5.1., b), 2), ii), l'article 1er, 7°, du présent arrêté définit les données personnelles comme « les nom et prénom ainsi que les adresses de facturation et de livraison de l'utilisateur final. »
La conservation des différentes adresses enregistrées auprès d'un opérateur, adresse(s) de livraison et de facturation, qui n'est pas prévue dans la directive, est demandée dans le présent arrêté pour les raisons suivantes.

Les adresses de livraison et de facturation ne sont pas toujours les mêmes. L'adresse de livraison (point de terminaison du réseau) est évidemment primordiale et indispensable. L'adresse de facturation est tout aussi essentielle car elle permet également de dépister la personne ou l'organisation qui paie l'abonnement. Les autorités ont constaté dans différents dossiers qu'une personne morale se chargeait de régler les factures des connexions téléphoniques ou Internet utilisées par des criminels. L'adresse de facturation a conduit les autorités à cette personne morale. Il convient d'observer que de nombreuses notions utilisées dans le présent arrêté royal ont été définies dans la LCE.

La définition de service de téléphonie reprise à l'article 126 de la LCE est ainsi d'application pour le présent arrêté.

Article 3

L'article 3 concerne les données que les fournisseurs de réseaux et services de téléphonie fixe accessibles au public, à l'exception de la téléphonie par Internet, doivent conserver.
La première catégorie de données (cf. supra et voir l'article 3, § 1er) vise entre autres les données fournies par l'abonné lors de la souscription de son abonnement, ou au cours de celui-ci. Les données d'identification de l'abonné ne dépendent pas de l'utilisation effective du service auquel il est abonné. Les autorités qui ont accès aux données conservées doivent pouvoir demander les données d'identification dès que l'abonnement est contracté, sans pour autant que l'abonné ait déjà effectivement utilisé ce service.

Les données visées à l'article 3, § 1er, 1° (le numéro attribué à l'utilisateur final) et 2° (les données personnelles de l'utilisateur final) correspondent à des données énumérées dans la directive (voir tableau de transposition). Il est renvoyé pour le surplus aux commentaires relatifs à l'article 1er, 7° (définition de « données personnelles »).

Les données visées à l'article 3, § 1er, 3° (la date de début de l'abonnement ou de l'enregistrement au service) et 5° (l'identité du fournisseur qui transfère le numéro et l'identité du fournisseur auquel le numéro est transféré) ne sont pas reprises dans la directive mais doivent être conservées pour les raisons suivantes.

Grâce à la libéralisation du marché des télécommunications, il est beaucoup plus facile pour les utilisateurs finals de téléphonie de changer d'opérateur tout en conservant leur numéro. Pour pouvoir s'informer auprès du bon opérateur, il importe que les services publics bénéficiaires de la conservation des données sachent précisément depuis quand l'utilisateur final est affilié à son opérateur actuel et quel était son opérateur d'origine en cas de transfert de numéro. Grâce à ces informations, les autorités (par exemple le juge d'instruction ou le procureur du Roi) peuvent adresser des réquisitions supplémentaires aux bons opérateurs. Demander des informations à un mauvais opérateur n'a, en effet, aucun sens. Ces données permettront donc d'interroger plus efficacement et de manière plus ciblée les opérateurs. Elles éviteront en outre des demandes inutiles auprès des opérateurs et les frais de justice plus élevés générés par celles-ci.

Il n'est pas suffisant de savoir que le numéro a été porté d'un opérateur à un autre. Encore faut-il savoir quand cela a eu lieu. Cela est possible en connaissant la date de début de l'abonnement ou de l'enregistrement au service. De plus, la durée qui s'écoule entre la souscription à l'abonnement et son utilisation active peut donner une indication sur le profil de l'utilisateur final, qui peut constituer un indice utile pour les autorités.

En ce qui concerne la portabilité des numéros, le fournisseur auquel un numéro est transféré devra

pouvoir fournir l'identité du fournisseur duquel il a reçu le numéro. Le fournisseur qui transfère le numéro doit également pouvoir identifier le fournisseur qui le reçoit. En d'autres termes, lorsqu'un numéro a été porté plusieurs fois, le dernier fournisseur à qui un numéro est transféré doit savoir de qui il reçoit ce numéro mais ne doit pas savoir qui est le premier fournisseur de la chaîne.
Les données visées à l'article 3, § 1er, 4° (le type de service de téléphonie fixe utilisé ainsi que les services annexes auxquels l'utilisateur final a souscrit) vont un peu plus loin que ce que prévoit la directive qui vise « le service téléphonique utilisé » (article 5.1., d), 1°), mais pas les services annexes.

Par « services annexes », on entend les services supplémentaires auxquels un client peut souscrire gratuitement, ou contre paiement. Par exemple : service de répondeur, fax, service SMS, déviation d'appel, formule particulière pour appeler à tarif avantageux certains numéros ou destinations, service de Calling Card, conversation à plusieurs, etc.

Ces services annexes fournissent aux autorités publics bénéficiaires de la conservation des données des indices utiles quant à l'utilité d'une demande d'information auprès d'un opérateur. Ainsi, à titre d'illustration, il est intéressant pour les autorités de savoir qu'un utilisateur final a souscrit à un service de déviation d'appel. Cela pourrait, par exemple, indiquer que les recherches des autorités doivent plutôt s'orienter vers le numéro vers lequel la déviation d'appel est effectuée.

Les données visées à l'article 3, § 1er, 6° (les données relatives au type de paiement ainsi qu'à l'identification et à la date de paiement de l'abonnement ou de l'utilisation du service) sortent du cadre des données visées par la directive mais représentent un réel intérêt dans le cadre d'une enquête, où ces quelques informations sont souvent la seule piste dont disposent les services de police afin de tenter d'identifier un suspect. Ces données de paiement sont parfois pour les autorités judiciaires et les services de renseignement et de sécurité la seule trace conduisant à l'utilisateur final d'un service de communications déterminé.

En effet, les abonnements télécom sont souvent souscrits sous un faux nom mais doivent néanmoins être payés. Il importe dès lors de conserver le numéro de compte ou de carte de paiement utilisé pour régler l'abonnement ou pour recharger le crédit d'utilisation.

Il est demandé aux opérateurs de conserver les données suivantes :

- type de paiement (virement, ATM, paiement par carte de crédit,...) ;
- identification du moyen de paiement (numéro de compte, numéro de carte de paiement,...) ;
- date et heure du paiement.

Il est demandé aux opérateurs de conserver les données de paiement des douze derniers mois afin de pouvoir également analyser l'unique trace éventuelle pouvant conduire à l'utilisateur final réel durant la période où les données de trafic sont conservées.

Les données demandées sont actuellement disponibles chez les opérateurs et sont régulièrement demandées par les autorités judiciaires. Ainsi, sur base des factures 2006 à 2011 contrôlées par le NTSU-CTIF et payées par la Justice aux opérateurs, on constate qu'il a été demandé aux opérateurs sur base des articles 46bis et 88bis du Code d'instruction criminelle en moyenne par an 309 fois une copie du contrat initial (pour déterminer le moyen de paiement), 446 fois une copie des factures (pour les mêmes raisons) et près de 5 500 fois des informations sur la recharge d'une carte prépayée (en vue de déterminer le lieu et moyen de paiement).

Ces données de paiement constituent donc pour le magistrat une trace susceptible de le mener à l'utilisateur final pour lequel il pourra ensuite ouvrir une enquête auprès des organismes bancaires concernés.

Les explications ci-dessus valent également pour les articles 4, 5 et 6.

La deuxième catégorie de données vise les données qui auront été générées lors d'une communication (voir l'article 3, § 2 et supra). Toutes les données visées au paragraphe 2 de l'article 3 sont reprises dans la directive (voir tableau de transposition).

S'il y a eu déviation d'appel, il est nécessaire que le fournisseur de réseau ou service de communications électroniques puisse fournir le numéro vers lequel l'appel a été dévié. De même, si plusieurs appels ont lieu simultanément, les données de trafic et les données de localisation doivent être fournies pour chaque numéro appelé ou appelant.

Également pour cette deuxième catégorie, une description du type de service utilisé doit permettre de déterminer s'il s'agit d'un appel vocal ou alternativement de l'envoi ou de la réception d'un fax (un fax est transporté par un canal vocal et les opérateurs ne sont généralement pas en mesure de distinguer un fax d'un appel vocal, sans regarder le contenu des communications, ce qui est interdit), de l'envoi ou de la réception d'un sms, etc. Par exemple, en cas d'utilisation d'une Calling Card, l'utilisation de cette carte et des données qui s'y rapportent (comme le lieu d'appel) devront être conservés.

Conformément à l'article 126, § 3, alinéa 3, de la LCE, l'article 3, § 3, de l'arrêté royal précise le point de départ pour le calcul du délai de conservation des données précitées.
Il en est de même pour l'article 4, § 3, l'article 5, § 3, et l'article 6, § 3, ci-après.

Article 4

L'article 4 concerne les données que les fournisseurs de réseaux ou services de téléphonie mobile accessibles au public, à l'exception de la téléphonie par l'internet, doivent conserver.
Les données visées à l'article 4, § 1er, 1° (le code IMSI), 2° (les données personnelles de l'utilisateur final) sont reprises dans la directive (voir tableau de transposition). Il est renvoyé pour le surplus aux commentaires relatifs à l'article 1er, 7° (définition de « données personnelles »).

Pour ce qui concerne les cartes prépayées, le présent arrêté royal n'a pas pour objet d'imposer aux fournisseurs ou aux points de vente d'obtenir les données personnelles visées à l'article 2, 7°, de l'utilisateur final lors de l'achat d'une carte prépayée. Une telle obligation n'a en effet pas sa place ici. Cependant, si le fournisseur dispose de ces données personnelles ou de certaines d'entre elles, il doit les conserver.

Pour ce qui concerne la date et le lieu de la souscription à l'abonnement ou de l'enregistrement de l'utilisateur final (article 4, § 1er, 3°) et la portabilité des numéros (article 4, § 1er, 6°), les commentaires de l'article 3 s'appliquent mutatis mutandis à l'article 4. On ajoutera que le lieu de la souscription à l'abonnement ou de l'enregistrement de l'utilisateur final est une donnée utile pour les autorités.

Vu les canaux commerciaux, l'abonnement peut être souscrit ou l'enregistrement peut être effectué dans un magasin, un phoneshop ou un bureau local, où la copie originale du contrat signé est généralement également conservée. Toutes les données personnelles qui y sont indiquées ne sont pas nécessairement transmises à l'opérateur. C'est pourquoi il est intéressant de savoir où

l'abonnement a été souscrit ou où l'enregistrement a eu lieu. Sur la base de l'écriture et de la signature, il est possible de vérifier si le contrat a réellement été conclu par la personne dont les coordonnées sont reprises dans le document ou si cette personne a été victime d'une usurpation d'identité.

Ce lieu est actuellement disponible chez les opérateurs et est régulièrement demandé par les autorités judiciaires. Ainsi, sur base des factures 2006 à 2011 contrôlées par le NTSU-CTIF et payées par la Justice aux opérateurs, on constate qu'il a été demandé aux opérateurs sur base des articles 46bis et 88bis du Code d'instruction criminelle en moyenne par an 60 fois le « point d'achat ».
Les données visées à l'article 4, § 1er, 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) correspondent au prescrit de la directive (voir article 5.1., e), 2), vi), qui limite néanmoins cette donnée aux services anonymes à pré-paiement.

Il est important de connaître avec exactitude le moment ainsi que l'endroit à partir desquels le service a été activé. Savoir quand la carte SIM a été achetée, et quand elle a été utilisée la première fois (3° et 4°) peut fournir des indices précieux aux enquêteurs. Cela vaut tant pour un abonnement régulier que pour un abonnement prépayé ou une carte prépayée. Par exemple, l'utilisation du service peut indiquer qu'un acte a été commis avec préméditation. L'absence d'utilisation du service peut indiquer un cas de fraude et une tentative de création d'une fausse identité.

Pour ce qui concerne les services annexes (article 4, § 1er, 5°), et les informations relatives au type de paiement (article 4, § 1er, 7°), données qui ne sont pas prévues dans la directive, les commentaires effectués à l'article 3 s'appliquent mutatis mutandis à l'article 4.

Par services annexes pour la téléphonie mobile, on entend les services supplémentaires auxquels un client peut souscrire gratuitement, ou contre paiement. Par exemple : service de répondeur, déviation d'appel, formule particulière pour appeler à tarif avantageux certains numéros ou destinations, conversation à plusieurs, etc. En ce qui concerne l'utilité de conserver ce type de données, il est renvoyé aux explications données pour l'article 3, § 1er, 4°.

Les données visées au paragraphe 2 de l'article 4 sont toutes reprises dans la directive, à l'exception de l'article 4, § 2, 6° et 7° de l'arrêté royal.

L'article 4, § 2, 6°, vise la localisation du point de terminaison du réseau au début et à la fin de chaque connexion. On rappellera que la téléphonie mobile diffère de la téléphonie fixe principalement au niveau de la localisation du point de terminaison de réseau qui sera différente pour chaque communication. La directive vise bien « l'identité de localisation (identifiant cellulaire) au début de la communication » (article 5, 1, f), 1)) et prévoit donc la conservation du point de terminaison au début de la communication. Il est souhaitable de l'étendre à la terminaison du réseau à la fin de la communication lorsque cette information est disponible.

En téléphonie mobile, il est courant que les gens se déplacent pendant la communication. Étant donné que la localisation de l'appel est souvent utilisée comme ébauche de preuve, il importe d'avoir une idée précise de l'endroit où cette communication a eu lieu. Si le point de terminaison à la fin de l'appel est disponible, il est important pour la justice de savoir où il se trouve.

Dans le passé, certains opérateurs belges ont adapté leur système pour pouvoir communiquer cette information, ce qu'ils font actuellement à la demande des autorités judiciaires.

Il est exigé d'enregistrer la localisation du point de terminaison du réseau au début et à la fin de chaque connexion, mais non pas au cours de cette connexion. En d'autres termes, lorsque l'utilisateur final se déplace en téléphonant, la localisation des mâts intermédiaires utilisés au cours de la connexion ne doit pas être enregistrée.

L'article 4, § 2, 7°, vise « 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 », alors que l'article 5.1, f), 2) de la directive vise « les données permettant d'établir la localisation géographique des cellules, en se référant à leur identité de localisation (identifiant cellulaire), pendant la période au cours de laquelle les données de communication sont conservées. » (c'est nous qui soulignons).

Il vaut mieux dire que les données de localisation des cellules doivent être conservées en prenant en compte cette localisation au moment où la communication a eu lieu. Cela permettra aux autorités de recevoir ces données de localisation telles qu'elles existaient au moment de la communication, mêmes si des modifications ont été faites dans l'architecture du réseau après la fin de la communication et ont modifié la localisation de ces cellules.

On rappellera à cet égard que la configuration d'un réseau mobile est assez dynamique. Fréquemment des antennes et des cellules sont reconfigurées ou déplacées. Un identifiant d'une cellule qui désigne une localisation à un moment donné peut être tout à fait différent 6 mois plus tard. D'où l'importance de connaître la configuration du réseau au moment de la communication. Par exemple si, au jour J, la cellule X du fournisseur concerné couvrait un périmètre déterminé, il se peut qu'au moment où les autorités compétentes demanderont l'accès aux données de localisation, la configuration du réseau ait été profondément modifiée. Il est donc nécessaire de pouvoir dire, à la date de la demande d'accès aux données, quel était le périmètre couvert au jour J, ce dernier ayant pu changer depuis.

Les données visées à l'article 4, § 1er, 8° (le numéro IMEI) sont reprises dans la directive (voir tableau de transposition).

Article 5

L'article 5 vise les fournisseurs de réseaux ou services offrant un accès à l'internet accessible au public, à l'exception du courrier électronique par l'internet accessible au public et de la téléphonie par l'internet accessible au public.

Les données visées à l'article 5, § 1er, 1° (l'identifiant de l'utilisateur final) et 2° (les données personnelles de l'utilisateur final) sont également reprises dans la directive (voir tableau de transposition). Il est renvoyé pour le surplus aux commentaires relatifs à l'article 1er, 7° (définition de « données personnelles »).

Les données visées à l'article 5, § 1er, 3° (la date et l'heure de la souscription à l'abonnement ou l'enregistrement de l'utilisateur final) et 4° (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) ne sont pas reprises dans la directive mais doivent être conservées pour les raisons suivantes.
Différents services d'accès à Internet permettent de s'enregistrer en ligne en tant que nouvel utilisateur final.

En l'absence de contact réel entre l'opérateur ou le fournisseur de service et le client, il est de plus en plus fréquent de voir l'utilisateur final encoder de fausses données d'identité. Pour permettre

l'identification réelle de l'utilisateur final, il faut en pareils cas conserver les traces laissées sur Internet (adresse IP, port source et point de terminaison du réseau lors de la création du compte). En plus de l'adresse IP, il est nécessaire de conserver le port source de la connexion ayant servi à la création de l'abonnement ou à l'enregistrement de l'utilisateur final pour les raisons suivantes. Jusqu'en 2011, une adresse IP utilisée à un certain moment permettait l'identification d'une seule personne.

Pour des raisons techniques et commerciales, un grand nombre de fournisseurs d'accès à internet ont récemment migré vers le partage d'une adresse IP entre plusieurs utilisateurs finals.

Afin de rendre cela possible, les 65 536 ports (TCP/UDP) disponibles pour une adresse IP sont divisés entre les différents utilisateurs finals de cette adresse IP.

La conservation des données a pour but d'identifier de manière précise et univoque l'utilisateur final internet impliqué dans un dossier judiciaire, et d'exclure les autres.

Pour différencier les différents utilisateurs finals d'Internet partageant une même adresse IP, et identifier de manière non ambiguë un certain utilisateur final (le suspect), il est nécessaire que le fournisseur d'accès à internet qui partage les adresses IP entre plusieurs utilisateurs finals conserve également pour chaque utilisateur final, à côté de l'adresse IP, les ports qui lui ont été attribués et la période de cette attribution.

Il faut rappeler à cet égard que la directive a été adopté le 15 mars 2006 et qu'à cette époque, les fournisseurs d'accès à Internet ne partageaient pas une adresse IP entre plusieurs utilisateurs finals. Il est donc logique que la directive n'ait pas pu prévoir la conservation des ports. Le présent arrêté prend en compte cette évolution technologique et économique en visant également les ports.

Les données visées à l'article 5, § 1er, 5° (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) ne sont pas reprises telles quelles dans la directive. On notera cependant que la directive vise « la ligne d'abonné numérique (DSL) ou tout autre point terminal de l'auteur de la communication » (article 5.1, e), 3), ii), de la directive), ce qui revient à demander l'identification du point de terminaison du réseau pour chaque communication. Les données à conserver en vertu de l'article 5, § 1er, 5°, ne constituent donc pas une charge supplémentaire importante pour les opérateurs.

Le point de terminaison du réseau correspond à l'identification de l'appareil utilisé pour la connexion. Il s'agit, entre autres, de l'adresse MAC du modem ou du routeur connecté au point de terminaison chez l'utilisateur final (numéro d'identification qui se compose d'une série de 12 chiffres et/ou lettres). Par contre, le présent arrêté royal n'oblige pas les opérateurs à identifier l'adresse MAC des équipements qui sont connectés chez l'utilisateur final à ce modem ou routeur, ce qui ne serait d'ailleurs pas possible dans bien des cas. L'identification du point de terminaison du réseau permet au fournisseur d'accès d'identifier son client et donc de lui attribuer une adresse IP grâce à laquelle il pourra établir sa connexion. En conservant uniquement l'adresse IP et les ports source sans conserver le point de terminaison du réseau, il ne serait pas possible de localiser l'utilisateur final.

Les données visées à l'article 5, 6° (les services annexes auxquels l'utilisateur final a souscrit auprès du fournisseur d'accès public à l'internet) ne sont pas reprises telles quelles dans la directive. Néanmoins, l'article 5.1, e), 3, ii) de la directive prévoit la conservation de « la ligne d'abonné numérique (DSL) ou tout autre point terminal de l'auteur de la communication ». Dans sa

communication au fournisseur, l'utilisateur final est donc amené à lui demander à s'abonner aux services annexes.

Il faut entendre par « services annexes auxquels l'utilisateur final a souscrit » les différentes possibilités ou formules offertes par l'opérateur à son client : telles qu'une bande passante plus importante, par exemple. Il est ainsi par exemple intéressant pour les autorités de savoir que l'utilisateur final a souscrit à un service similaire à Skype, mais offert par le fournisseur de l'accès à Internet, ce qui pourrait indiquer que les recherches doivent s'orienter vers les communications sur ce type de service.

Les données visées à l'article 5, § 1er, 7° (les données relatives au type de paiement ainsi qu'à l'identification et à la date du paiement de l'abonnement ou de l'utilisation du service) ne sont pas prévues par la directive. Il est renvoyé aux explications données à l'article 3 à ce égard.

Les données visées à l'article 5, § 2, 1° (l'identifiant de l'utilisateur final) sont prévues par la directive (voir tableau de transposition).

Les données visées à l'article 5, § 2, 2°, (a) l'adresse IP et 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) vont un peu plus loin que ce que prévoit la directive qui vise notamment « l'adresse IP (protocole internet), qu'elle soit dynamique ou statique, attribuée à une communication par le fournisseur d'accès à l'internet » (article 5, 1, c), 2, i)).

Comme il a été ci-dessus (voir commentaires relatifs à l'article 5, § 1er, 4°), vu que plusieurs fournisseurs partagent une adresse IP entre plusieurs utilisateurs finals, il n'est plus suffisant de conserver cette adresse IP mais également les ports sources.

Les données visées à l'article 5, § 2, 3° (l'identification et la localisation du point de terminaison du réseau utilisé par l'utilisateur final au début et à la fin d'une connexion) vont un peu plus loin que la directive qui ne prévoit la conservation de ces données que pour le début d'une connexion (voir l'article 5, 1, f), 1) de la directive).

Grâce aux nouvelles technologies il est possible de se connecter sans fil à l'internet (p.ex en « Wifi » ou Internet mobile) depuis n'importe quelle localisation couverte par un réseau sans fil. Il existe également des standards wi-fi qui permettent à l'utilisateur final de se déplacer lors de sa connexion au réseau et qui permettent à cette connexion d'être continue car passant d'une antenne à une autre. Il est donc utile de préciser ici que si l'utilisateur final se déplace durant la connexion et que celle-ci passe d'une station de base ou d'une antenne à une autre, le fournisseur de réseau ou service de communications électroniques offrant un accès à l'internet accessible au public devra être capable de communiquer la localisation de l'utilisateur final au début et à la fin de la connexion, comme c'est le cas dans le cadre de la téléphonie mobile. La localisation de l'utilisateur final pendant la connexion ne doit par contre pas être conservée, ce qui signifie que lorsque l'utilisateur final se déplace pendant la communication, la localisation des mats ou stations de base intermédiaires ayant servi à la connexion ne doit pas être conservée.

L'identification et la localisation du point de terminaison du réseau utilisé par l'utilisateur final au début et à la fin d'une connexion permettra de déterminer d'où à où cet utilisateur final s'est déplacé, ce qui peut constituer des informations utiles pour les autorités.

Les données visées à l'article 5, § 2, 4° (la date et l'heure d'ouverture et de la fermeture d'une session

du service d'accès à l'internet) sont prévues par la directive (voir tableau de transposition).
A l'article 5, § 2, 5°, il est demandé aux fournisseurs de conserver le volume de données envoyées vers le réseau et téléchargées pendant la durée de la session ou autre unité de temps demandée.
En d'autres termes, il est demandé aux fournisseurs de conserver, par durée de connexion (ou autre unité de temps, qui pourrait être la durée pendant laquelle une adresse IP précise a été attribuée), le volume de données téléchargées ou uploadées.

Ces données ne sont pas reprises dans la directive mais la conservation de ces dernières est justifiée comme suit.

Tout d'abord, depuis l'apparition des connexions à large bande avec tarif mensuel fixe et des réseaux wifi pour utilisateurs finals à domicile, les utilisateurs finals restent de plus en plus souvent connectés à Internet 24 heures sur 24. Pour pouvoir fournir les données de connexion et procéder à une évaluation de la faisabilité technique d'une interception internet, il est important pour les enquêteurs de pouvoir se faire une idée de l'activité effective de la connexion internet concernée.
Ensuite, connaître l'activité d'une personne peut également permettre aux enquêteurs et au juge de décider s'il est opportun de faire une interception de la ligne utilisée. En effet, s'il n'y a aucune activité, il ne sera pas productif d'effectuer une interception et dès lors, des frais de justice inutiles seront évités.

Par ailleurs, ces données sont actuellement conservées systématiquement par les fournisseurs dans leurs données clients.

Finalement, l'activité d'une personne peut, en partie, être déduite des volumes de données uploadés et downloadés.

Si, par exemple, une adresse IP apparaît lors de l'identification des connexions sur un site pédopornographique, il sera utile de savoir si cette personne est plutôt active (upload de fichiers - quelle taille), ou si elle télécharge de gros volume de fichiers mis à disposition (plutôt consommatrice).

Connaître son activité up/download au moment où son adresse IP a été utilisée pourra être utile.
En d'autres termes, un des buts de la conservation des données relatives au volume de données téléchargées ou uploadées est de pouvoir analyser le comportement de la personne si celle-ci est soupçonnée de comportement illicite.

A contrario, voir que cette personne n'a pas utilisé sa capacité de téléchargement ou d'upload pourrait également la disculper.

Les données visées à l'article 5, § 2, 6° (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) correspondent à l'article 5.1, f), 2), de la directive. Cette dernière se réfère cependant à l'identifiant cellulaire des cellules « pendant la période au cours de laquelle les données de communications sont conservées » alors que le présent arrêté se réfère à l'identifiant cellulaire des cellules au moment où la communication a été effectuée. Il est renvoyé à cet égard à l'explication donnée ci-dessus par rapport à l'article 4, § 2, 7°.

Le paragraphe 3 de l'article 5 fixe le point de départ du délai de conservation conformément à l'article 126, § 3, de la LCE. Ce dernier article stipule en son alinéa 1er que « Les données visant à identifier les utilisateurs finals, le service de communications électroniques utilisé et l'équipement

terminal qui est présumé avoir été utilisé sont conservées à partir de la souscription au service, aussi longtemps qu'une communication entrante ou sortante est possible à l'aide du service souscrit et pendant douze mois à compter de la date de dernière communication entrante ou sortante enregistrée. »

Lorsqu'un service d'accès à l'internet est utilisé, une communication se crée toujours entre l'utilisateur final et le serveur du fournisseur de service d'accès à internet. Dans le contexte du service d'accès à l'internet, la communication entrante ou sortante mentionnée dans l'article 126, § 3, de la LCE, est donc la communication avec le serveur et donc en pratique l'utilisation du service d'accès à l'internet.

Article 6

L'article 6 vise les données à conserver par les fournisseurs de services de courrier électronique par internet accessibles au public et par les fournisseurs de services de téléphonie par internet accessibles au public, à l'exception de l'accès à l'internet accessible au public.

En ce qui concerne les services de courriers électroniques, on vise tant les courriers SMTP que les webmails, pour autant qu'ils soient offerts en Belgique.

Il existe différentes formes de téléphonie qui utilisent le protocole Internet; on parle souvent de « Voice over IP » (« VoIP »). La téléphonie par internet suppose qu'un ou les deux participants à la communication utilisent un logiciel spécial afin qu'un ordinateur puisse entrer en contact avec un autre. Lorsque seul l'appelant utilise un logiciel spécifique permettant à un ordinateur d'entrer en contact avec un correspondant en utilisant un numéro de téléphone, l'appelant doit établir une connexion via son fournisseur de service avec le réseau téléphonique classique. Dans ce même exemple, l'article 6 s'applique pour ce qui concerne la partie téléphonie par internet.

Les données visées à l'article 6, § 1er, 1° (l'identifiant de l'utilisateur final) et 2° (les données personnelles de l'utilisateur final) sont également prévues dans la directive (voir tableau de transposition). Il est renvoyé pour le surplus aux commentaires relatifs à l'article 1er, 7° (définition de « données personnelles »).

Les données visées à l'article 6, § 1er, 3° (la date et l'heure de la création du compte de courrier électronique ou de téléphonie par Internet) ne sont pas reprises dans la directive.

En ce qui concerne les comptes mails activés par défaut lors de la souscription d'un abonnement chez un fournisseur d'accès, certaines des données mentionnées au paragraphe 1er (telles que les date et heure de création du compte) sont déjà conservées par les opérateurs en pratique dans le cadre de la souscription à un abonnement ou à un enregistrement à un service et ne doivent pas être conservées séparément. Ainsi, par exemple, les date et heure de création du compte coïncideront avec les date et heure de souscription de l'abonnement. Il ne s'agit donc pas d'une charge lourde supplémentaire pour les opérateurs.

En revanche, si l'utilisateur final demande l'ouverture d'une seconde adresse e-mail, ou crée un second alias, ces données devront être conservées au même titre que la création d'un nouveau compte.

La conservation de la date et de l'heure de la création du compte de courrier électronique ou de téléphonie par internet est utile pour les raisons suivantes. La durée qui s'écoule entre la souscription au compte et son utilisation active peut donner une indication sur le profil de

l'utilisateur final, qui peut constituer un indice utile pour les autorités. Un compte qui n'est pas utilisé ou de manière très sporadique peut être un indice de fraude ou de création d'une fausse identité électronique.

Les données visées à l'article 6, § 1er, 4° (l'adresse IP et le port source ayant servi à la création du compte de courrier électronique ou de téléphonie par l'internet) ne sont pas reprises dans la directive.

Comme expliqué ci-dessus pour ce qui concerne l'article 5, § 1er, 4°, en l'absence de contact réel entre l'opérateur ou le fournisseur de service et le client, il est de plus en plus fréquent de voir l'utilisateur final encoder de fausses données d'identité. Pour permettre l'identification réelle de l'utilisateur final, il faut en pareils cas conserver les traces laissées sur Internet (adresse IP, port source et point de terminaison du réseau lors de la création du compte).

Par exemple, si un utilisateur final d'Internet crée une boîte à messages internet sur mail.be au nom d'une personnage de fiction habitant dans un lieu imaginaire, les « données personnelles » enregistrées ne sont d'aucune utilité. L'adresse IP de cet utilisateur final, le port source, ainsi que la date et l'heure de la création de son « abonnement » sont les seules données fiables pouvant conduire les autorités au véritable utilisateur final.

Cela doit contribuer à éviter qu'une « identification » basée sur les « données personnelles » nous mène à la mauvaise personne. En effet, si l'enregistrement n'était pas fait au nom du personnage de fiction mais au nom d'une personne existante et à son insu, il ne serait pas évident de repérer le caractère erroné de ces données personnelles.

Les données visées à l'article 6, § 1er, 5° (les données relatives au paiement ainsi qu'à l'identification et à la date du paiement de l'abonnement ou de l'utilisation du service) ne sont pas reprises dans la directive. Il est renvoyé aux explications pour l'article 3, § 1er, 6°.

Les données visées à l'article 6, § 2 sont reprises dans la directive. Néanmoins, l'article 6, § 2, 3° de l'arrêté royal ne correspond pas exactement au prescrit de la directive.

En effet, cet article prévoit la conservation de « a) l'adresse IP et le port source utilisés par l'utilisateur final et b) l'adresse IP et le port source utilisé par le destinataire ».

La directive ne vise quant à elle que la conservation de l'adresse IP (voir article 5, 1, c), 2, i).

Pour ce qui concerne la conservation des ports, il est renvoyé aux explications ci-dessus données par rapport à l'article 5, § 1er, 4° et § 2, 2°.

Le paragraphe 3 de l'article 6 prévoit que les données d'identification doivent être conservées aussi longtemps qu'une communication entrante ou sortante est possible. Une communication sera possible aussi longtemps qu'un compte existe.

Article 7

Le premier alinéa vise les fournisseurs de différents services de communications électroniques de façon combinée, tel que par exemple l'envoi d' e-mails via un téléphone mobile intelligent (« Smart Phone ») qui permet également d'offrir des services de téléphonie mobile classique.
Dans ce même exemple le fournisseur devra conserver les données correspondant tant au paragraphe 2 de l'article 4 (téléphonie mobile) qu'à celles du paragraphe 2 de l'article 6 (courrier

électronique).

Dans l'exemple visé à l'article 6, il y a clairement l'utilisation d'un service de téléphonie par l'internet qui est combiné avec un service de téléphonie fixe ou mobile. Pour ce qui concerne le service de téléphonie par l'internet, l'article 6 est d'application alors que pour la téléphonie fixe ou mobile, c'est respectivement l'article 3 ou 4 qui s'applique.

En vue de l'administration de la preuve, il est nécessaire que tous les fournisseurs de communications électroniques visés utilisent la même indication de l'heure. Actuellement, de nombreuses horloges des systèmes utilisés par les fournisseurs n'indiquent pas une heure conforme à l'heure officielle. Cela peut entraîner des problèmes pour l'administration de la preuve si les données des différents fournisseurs doivent être comparées entre elles. C'est pourquoi le présent article prévoit que les horloges utilisées dans les systèmes des fournisseurs doivent être synchronisées avec le signal horaire GPS.

Article 8

L'article 8 institue, au sein de chaque Cellule Coordination Justice, un préposé à la protection des données, comme le permet l'article 17bis, alinéas 2 et 3, 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. Par ailleurs, cette mesure spécifique vise à protéger et sécuriser les données comme l'exige l'article 7 de la directive.

L'article 8, alinéa 3, vise à garantir l'indépendance du préposé dans ses fonctions.

Dans son premier avis (avis n° 24/2008 du 2 juillet 2008), la commission de la vie privée avait demandé que lui soient communiqués de manière systématique les avis et rapports des préposés à la protection des données, la nature du lien juridique entre ces préposés et le service dans lequel ils exerceront leur fonction de préposé, tous les éléments concernant les qualifications professionnelles relatives à la fonction de préposé et les mesures prises par le responsable du traitement en fonction des missions que doit exercer le préposé à la protection des données.

Ces recommandations de la commission de la vie privée n'ont cependant pas été suivies dans le présent arrêté, dès lors que la communication des données susmentionnées risque de créer une charge administrative conséquente tant pour les fournisseurs que pour la commission de la vie privée.

La commission disposera de la possibilité de prendre contact avec les préposés pour leur demander les informations qu'elle souhaite lorsque cela est nécessaire.

Article 9

L'article 9 donne obligation aux fournisseurs concernés de communiquer annuellement à l'Institut un certain nombre d'informations statistiques qui seront destinées au ministre qui a les communications électroniques dans ses attributions et au ministre de la Justice. Les ministres compétents font en sorte que ces données, conformément à l'article 10 de la directive, soient transmises à la Commission européenne.

Articles 10 et 11

Aucune règle particulière n'est prévue pour l'entrée en vigueur du présent arrêté. Cependant, une disposition transitoire donne un délai de douze mois aux fournisseurs pour mettre en place les

systèmes nécessaires pour conserver les données. De la sorte, les fournisseurs qui parviennent à mettre en place l'infrastructure nécessaire pour conserver les données visées aux articles 3 à 6 du présent arrêté avant le délai de douze mois peuvent conserver légalement ces données.

Nous avons l'honneur d'être,

Sire,
de Votre Majesté,
les très respectueux
et très fidèles serviteurs,
Le Ministre de l'Économie, J. VANDE LANOTTE
La Ministre de la Justice, Mme A. TURTELBOOM

19 septembre 2013 - Arrêté royal portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques

PHILIPPE, Roi des Belges,
A tous, présents et à venir, Salut.

Vu la loi du 13 juin 2005 relative aux communications électroniques, l'article 126, tel que modifié par la loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité et 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 ;

Vu les avis de l'Institut belge des services postaux et des télécommunications, donnés les 18 juin 2008, 7 juillet 2008 et 12 mars 2013 ;

Vu les avis de la Commission de la protection de la vie privée, n° 24/2008, donné le 2 juillet 2008 et n° 20/2009, donné le 1er juillet 2009 ;

Vu l'avis de l'Inspecteur des Finances du SPF Économie, donné le 14 mars 2013 ;

Vu l'avis de l'Inspecteur des Finances du SPF Justice, donné le 18 mars 2013 ;

Vu l'accord du Ministre du Budget, donné le 25 mars 2013 ;

Vu la consultation du 29 mars 2013 au 9 avril 2013 du Comité interministériel des Télécommunications et de la Radiodiffusion et la Télévision ;

Vu l'accord du Comité de concertation du 24 avril 2013 ;

Vu l'avis n° 53.841/2/V du Conseil d' État, donné le 26 août 2013, en application de l'article 84, § 1er, alinéa 1er, 1°, des lois sur le Conseil d'État, coordonnées le 12 janvier 1973 ;

Sur la proposition du Ministre de l'Économie et de la Ministre de la Justice et de l'avis des Ministres qui en ont délibéré en Conseil,

Nous avons arrêté et arrêtons :

Article 1er. 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 ») 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 communications électroniques (directive « vie privée et communications électroniques »).

Art. 2. Pour l'application de présent arrêté, il y a lieu d'entendre par :

1. « Loi » : la loi du 13 juin 2005 relative aux communications électroniques ;
2. « Institut » : l'Institut belge des services postaux et des télécommunications, tel que visé à

l'article 13 de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges ;
3. « Ministre » : le ministre ou le secrétaire d'État qui a les télécommunications dans ses attributions ;
4. « Arrêté royal du 9 janvier 2003 » : l'arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques ;
5. « Identifiant d'un utilisateur final » : l'identifiant exclusif attribué aux personnes qui s'abonnent ou s'inscrivent à un service d'accès à l'Internet ou à un service de communication par l'Internet ;
6. « Identifiant cellulaire » : le numéro d'identification de la cellule où un appel de téléphonie mobile a commencé ou a pris fin ;
7. « Données personnelles » : les nom et prénom ainsi que les adresses de facturation et de livraison de l'utilisateur final.

Art. 3. § 1er. Pour ce qui concerne les données relatives à l'identification de l'utilisateur final, de l'équipement terminal qui est présumé avoir été utilisé et du service de communications électroniques utilisé, les fournisseurs de services de téléphonie fixe accessibles au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent les données suivantes :

1. le numéro attribué à l'utilisateur final ;
2. les données personnelles 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.

§ 2. Pour ce qui concerne les données relatives au trafic et à la localisation, les fournisseurs de services de téléphonie fixe accessibles au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent 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.

§ 3. Les données visées au paragraphe 1er sont soumises à l'article 126, § 3, alinéa 1er, de la loi. Les données visées au paragraphe 2 sont soumises à l'article 126, § 3, alinéa 2, de la loi.

Art. 4. § 1er. Pour ce qui concerne les données relatives à l'identification de l'utilisateur final, de l'équipement terminal qui est présumé avoir été utilisé et du service de communications électroniques utilisé, les fournisseurs d'un service de téléphonie mobile accessible au public 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 ») ;
2. les données personnelles de l'utilisateur final ;
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 mobile de l'utilisateur final (« International Mobile Equipment Identity », « IMEI »).

§ 2. Pour ce qui concerne les données relatives au trafic et à la localisation, les fournisseurs d'un service de téléphonie mobile accessible au public et les fournisseurs de réseaux publics de communications électroniques sous-jacents conservent 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 ») de l'appelant et de l'appelé ;
4. l'identité internationale d'équipement mobile (« International Mobile Equipment Identity », « IMEI ») 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.

§ 3. Les données visées au paragraphe 1er sont soumises à l'article 126, § 3, alinéa 1er, de la loi.

Les données visées au paragraphe 2 sont soumises à l'article 126, § 3, alinéa 2, de la loi.

Art. 5. § 1er. Pour ce qui concerne les données relatives à l'identification de l'utilisateur final, de l'équipement terminal qui est présumé avoir été utilisé et du service de communications électroniques 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 les données suivantes :

1. l'identifiant de l'utilisateur final ;
2. les données personnelles de l'utilisateur final ;
3. la date et l'heure de la souscription à l'abonnement ou de l'enregistrement de l'utilisateur final ;
4. 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 ;

5. 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 ;
6. les services annexes auxquels l'utilisateur final a souscrit auprès du prestataire d'accès Internet public concerné ;
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.

§ 2. Pour ce qui concerne les données relatives au trafic et à la localisation, 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 ;
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. l'identification et la localisation du point de terminaison du réseau utilisé par l'utilisateur final au début et à la fin d'une connexion ;
4. la date et l'heure de l'ouverture et de la fermeture d'une session du service d'accès à l'internet ;
5. le volume de données envoyées vers le réseau et téléchargées pendant la durée de la session ou autre unité de temps demandée ;
6. 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.

§ 3. Les données visées au paragraphe 1er sont soumises à l'article 126, § 3, alinéa 1er, de la loi. Les données visées au paragraphe 2 sont soumises à l'article 126, § 3, alinéa 2, de la loi.

Art. 6. § 1er. Pour ce qui concerne les données relatives à l'identification de l'utilisateur final, de l'équipement terminal qui est présumé avoir été utilisé et du service de communications électroniques utilisé, 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 ;
2. les données personnelles de l'utilisateur final ;
3. la date et l'heure de la création du compte de courrier électronique ou de téléphonie par internet ;
4. l'adresse IP et le port source ayant servi à la création du compte de courrier électronique ou de téléphonie par l'internet ;
5. 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.

§ 2. Pour ce qui concerne les données relatives au trafic et à la localisation, 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.

§ 3. Les données visées au paragraphe 1er sont soumises à l'article 126, § 3, alinéa 1er, de la loi. Les données visées au paragraphe 2 sont soumises à l'article 126, § 3, alinéa 2, de la loi.

Art. 7. § 1er. Les fournisseurs de réseaux ou de services qui utilisent conjointement différents services conservent toutes les données relatives aux différents services utilisés, conformément aux articles 3 à 6.

La combinaison des données enregistrées doit permettre d'établir la relation entre l'origine de la communication et sa destination.

§ 2. Les heures qui doivent être enregistrées conformément aux articles 3 à 6 du présent arrêté doivent, en se référant au système de la division du jour en 24 heures, être précises à la seconde près. L'indication de l'heure doit toujours se faire par référence au fuseau horaire auquel la Belgique appartient et en tenant compte des périodes de l'heure d'été et de l'heure d'hiver.

Les fournisseurs précités doivent synchroniser l'horloge de leurs systèmes utilisés pour l'enregistrement de toutes les heures mentionnées dans le présent arrêté avec le signal horaire GPS.

Art. 8. § 1er. Chaque fournisseur désigne parmi les membres de la Cellule de Coordination de Justice, visée à l'article 2 de l'arrêté royal du 9 janvier 2003, un préposé à la protection des données à caractère personnel.

Dans l'exercice de ses missions, le préposé à la protection des données à caractère personnel agit en toute indépendance, et a accès à toutes les données visées par le présent arrêté qui sont traitées par le fournisseur ainsi qu'à tous les locaux pertinents du fournisseur.

L'exercice de ses missions ne peut entraîner pour le préposé des désavantages. Il ne peut, en particulier, être licencié ou remplacé comme préposé à cause de l'exécution des tâches qui lui sont confiées, sans motivation approfondie.

Le préposé à la protection des données veille à ce que les traitements effectués par la cellule Coordination Justice soient exécutés conformément à la loi.

Le préposé doit être placé à un niveau de la hiérarchie tel qu'il ait la possibilité de communiquer directement avec le management ou le comité de direction et d'exercer sa mission directement auprès du responsable du traitement.

§ 2. En particulier, il veille à ce que :

1. les traitements poursuivent les finalités décrites à l'article 126 de la loi ;
2. pour l'application du présent arrêté, seules les données décrites ci-dessus soient conservées

pour les finalités prévues ;
3. seules les catégories de personnes autorisées en vertu de l'article 126 de la loi et du présent arrêté aient accès aux données ;
4. les mesures de protection des données décrites dans l'article 126 de la loi soient respectées.

Art. 9. Au plus tard le 1er mars de chaque année, les fournisseurs de services et de réseaux communiquent à l'Institut les informations statistiques anonymes suivantes :

a) le nombre de cas dans lesquels des données ont été, au cours de la dernière année civile écoulée, transmises aux autorités compétentes ;
b) pour chaque donnée transmise, le délai écoulé entre la date à partir de laquelle les données ont été conservées et la date à laquelle les autorités compétentes ont demandé leur transmission ;
c) les cas dans lesquels des demandes de données n'ont pu être satisfaites.

L'Institut transmet ces informations annuellement au ministre et au Ministre de la Justice.

Art. 10. Les fournisseurs de services et de réseaux doivent être en mesure de conserver les données visées aux articles 3 à 6 au plus tard le premier jour qui suit l'expiration d'un délai d'un an prenant cours le jour de la publication du présent arrêté au Moniteur belge.

Art. 11. Le ministre qui a les Télécommunications dans ses attributions est chargé de l'exécution du présent arrêté.

Donné à Bruxelles, le 19 septembre 2013.

PHILIPPE

Par le Roi :
Le Ministre de l'Économie, J. VANDE LANOTTE
La Ministre de la Justice, Mme A. TURTELBOOM

Avis du Conseil d'État (53.841/2/V) du 26 août 2013 sur un projet d'arrêté royal « portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques »

Le 23 juillet 2013, le Conseil d'État, section de législation, a été invité par le Vice-Premier Ministre et Ministre de l'Économie, des Consommateurs et de la Mer du Nord à communiquer un avis, dans un délai de trente jours prorogé jusqu'au 29 août 2013 [1], sur un projet d'arrêté royal « portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques ».

Le projet a été examiné par la deuxième chambre des vacations le 26 août 2013. La chambre était composée de Robert Andersen, premier président du Conseil d'État, Pierre Vandernoot et Michel Pâques, conseillers d'État, Yves De Cordt, assesseur et Anne-Catherine Van Geersdaele, greffier.
Le rapport a été présenté par Laurence Vancrayebeck, auditrice.

La concordance entre la version française et la version néerlandaise a été vérifiée sous le contrôle de Pierre Liénardy, président de chambre.

L'avis, dont le texte suit, a été donné le 26 août 2013.

Comme la demande d'avis est introduite sur la base de l'article 84, § 1er, alinéa 1er, 1° , des lois coordonnées sur le Conseil d'État, tel qu'il est remplacé par la loi du 2 avril 2003, la section de législation limite son examen au fondement juridique du projet, à la compétence de l'auteur de l'acte ainsi qu'à l'accomplissement des formalités préalables, conformément à l'article 84, § 3, des lois coordonnées précitées.

Sur ces trois points, le projet appelle les observations suivantes.

Formalités préalables

Il ne ressort d'aucune des pièces communiquées au Conseil d'Etat que l'examen préalable de la nécessité de procéder à une évaluation d'incidence au sens de l'article 19/1 de la loi du 5 mai 1997 `relative à la coordination de la politique fédérale de développement durable' a bien été réalisé.
Si ce n'est chose faite, cet examen préalable devra donc encore être accompli, ainsi que, s'il y a lieu, l'évaluation d'incidence subséquente.

Observations générales

1. L'arrêté en projet vise à exécuter l'article 126 de la loi du 13 juin 2005 « relative aux communications électroniques », tel que remplacé par l'article 5 de la loi « 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 » [2], afin de transposer partiellement la Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 « sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications électroniques, et modifiant la Directive 2002/58/CE » (ci-après, la Directive 2006/24/CE).

Plusieurs dispositions de l'arrêté en projet prévoient la conservation de données qui ne figurent pas

1 Par courriel du 25 juillet 2013

2 Cette loi a été adoptée par le Parlement en date du 18 juillet 2013 (Doc. parl., Sénat., 2012-2013, n° 2222/4 et Doc. parl., Chambre, 2012-2013, n° 2921/6). Selon les informations transmises par le délégué du ministre, elle devrait bientôt être transmise au Roi pour sanction et promulgation.

dans la liste des données à conserver prévue par l'article 5 de la Directive 2006/24/CE. Il convient à cet égard de renvoyer à l'avis 53.272/4 donné le 27 mai 2013 sur l'avant-projet devenu la loi précitée, dans lequel le Conseil d'État s'est interrogé sur la question de savoir si le législateur pouvait prévoir la conservation de certaines données dans des buts qui dépassent les finalités prévues par la Directive 2006/24/CE. À ce propos, la section de législation a notamment observé ce qui suit :

> Il résulte des considérations qui précèdent que les États membres peuvent prévoir, sur la base de la Directive 2002/58/CE, des systèmes imposant aux opérateurs de conserver des données dans des buts qui dépassent celui prévu par la Directive 2006/24/CE, tout en respectant toutefois certaines conditions, étant celles fixées par l'article 15 de la Directive 2002/58/CE.
>
> C'est le système retenu par l'article 126 en projet : cette disposition non seulement transpose certes la Directive 2006/24/CE, mais en outre, en tant qu'elle dépasse l'objectif lié aux « infractions graves » assigné par cette directive, elle fait écho et trouve appui sur l'article 15 de la Directive 2002/58/CE.
>
> Il reste que, vu la complexité du droit européen et, pour reprendre les termes de la Commission européenne, vu « la relation juridique compliquée » entre la Directive 2006/24/CE et la Directive 2002/58/CE, il est permis de se demander si la solution qui serait la plus de nature à garantir le respect du droit européen ne consisterait pas à mettre en place deux systèmes parallèles, l'un transposant la Directive 2006/24/CE, l'autre s'appuyant sur la Directive 2002/58/CE. A cet égard, la section de législation observe par ailleurs que les considérants 15 et 16 du préambule de la Directive 2006/24/CE mentionnent que « la Directive 95/46/CE et la Directive 2002/58/CE sont pleinement applicables aux données conservées conformément à la [Directive 2006/24/CE] ».
>
> Quoi qu'il en soit, dès lors que l'auteur de l'avant-projet a opté pour un système qui s'appuie sur les deux directives précitées, il est tenu de respecter le double cadre juridique européen auquel il est fait écho.

Selon l'article 15 de la Directive 2002/58/CE, les États membres peuvent prévoir la conservation de données pendant une durée limitée pour autant qu'il s'agisse d'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 ».

À cet égard, le rapport au Roi contient de nombreux développements qui semblent pouvoir justifier que certaines données, bien que non mentionnées à l'article 5 de la Directive 2006/24/CE, soient conservées dans l'un des buts énumérés à l'article 126, § 2, de la loi précitée du 13 juin 2005.

2. A plusieurs reprises, l'arrêté en projet reproduit ou paraphrase des dispositions de l'article 126 de la loi précitée du 13 juin 2005.

Tel est notamment le cas de l'article 3 du projet - qui reproduit l'article 126, § 1er, alinéa 6, de la loi - et des articles 4, § 3, 5, § 3, 6, § 3 et 7, § 3, du projet - qui paraphrasent l'article 126, § 3, alinéas 1er et 2, de la loi. Ces dispositions seront dès lors omises.

Il n'appartient en effet pas au Roi de reproduire, dans un arrêté réglementaire, une règle déjà inscrite

dans une disposition législative. Pareil procédé peut induire en erreur sur la nature de la règle en question. Il laisse par ailleurs à penser qu'il est au pouvoir du Roi de modifier cette règle alors que ce pouvoir appartient au seul législateur.

3. L'article 126, § 1er, alinéa 1er, de la loi précitée du 13 juin 2005 impose aux fournisseurs de services ou de réseaux de communications électroniques qui y sont cités de conserver, notamment, des données « d'identification d'utilisateurs finals ». L'alinéa 4 de la même disposition habilite en outre le Roi à déterminer plus précisément les données qui entrent dans cette catégorie.

L'arrêté en projet ne se réfère pas à l'identification « d'utilisateurs finals », mais bien à l'identification « de l'abonné ou de l'utilisateur » [3]. Ces trois notions - utilisateur, utilisateur final et abonné - sont respectivement définies par l'article 2, 12°, 13° et 15°, de la loi précitée du 13 juin 2005. Il ressort de ces définitions que la notion d'utilisateur est plus large que celle d'utilisateur final. Il n'est pas admissible qu'en ce qui concerne la conservation de données d'identification, l'arrêté en projet ait un champ d'application plus large que celui prévu par l'article 126 de la loi précitée du 13 juin 2005.

Il n'est pas certain que telle soit l'intention de l'auteur du projet. En effet, à plusieurs reprises, s'agissant d'énumérer les données qui permettent d'identifier « l'abonné ou l'utilisateur », l'arrêté en projet fait référence à l'utilisateur « enregistré », c'est-à-dire l'utilisateur qui s'est enregistré auprès d'un opérateur, par opposition à l'utilisateur qui lui aurait souscrit un abonnement. Si l'intention est donc uniquement de distinguer, parmi les utilisateurs finals, ceux qui sont abonnés et ceux qui sont enregistrés, l'arrêté en projet devrait être rédigé en ce sens.

Observations particulières

Préambule

A l'alinéa 1er, même si la directive mentionnée contribue à déterminer le cadre juridique du projet, elle n'en constitue pas le fondement légal.

L'alinéa 1er sera omis.

Dispositif

Article 2

L'article 2, 5°, de l'arrêté en projet, définit l'« identifiant d'un utilisateur » comme étant « l'identifiant exclusif attribué aux personnes qui s'abonnent ou s'inscrivent à un service d'accès à l'Internet ou à un service de communication par l'Internet ».

Or, dans les articles 6 et 7 de l'arrêté en projet, qui ont trait aux services d'accès à l'internet et aux services de communication par internet, il n'est pas fait référence à l'identifiant d'un utilisateur, mais bien à l'identifiant « de l'abonné ou de l'utilisateur ».

Selon le rapport au Roi, la définition de l'identifiant d'un utilisateur est une transposition d'un concept défini à l'article 2 de la Directive 2006/24/CE. Or, dans cet article, la notion utilisée est celle de « numéro d'identifiant », défini comme étant « le numéro d'identification exclusif attribué aux personnes qui s'abonnent ou s'inscrivent à un service d'accès à l'internet ou à un service de communication par l'internet ».

3 Voir les articles 4, § 1er, 5, § 1er, 6, § 1er, et 7, § 1er, du projet.

Mieux vaut dès lors utiliser cette notion de numéro d'identifiant tant à l'article 2, 5°, qu'aux articles 6 et 7 du projet.

Le greffier, Anne-Catherine Van Geersdaele
Le premier président, Robert Andersen