Avis n° 20/2009 du 1er juillet 2009

Objet: demande d'avis relatif à l'avant-projet de loi et au projet d'arrêté royal en matière de rétention de données et au projet d'arrêté royal relatif à l'obligation de collaboration (A/09/012)

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 LVP), en particulier l'article 29 ;

Vu la demande d'avis du Ministre de la Justice, Monsieur Stefaan De Clerck, reçue le 23/04/2009;

Vu le rapport de Monsieur le Président ;

Émet, le 1er juillet 2009, l'avis suivant :

A. INTRODUCTION

1. Le 23 avril 2009, le Ministre de la Justice a demandé à la Commission d'émettre un avis d'urgence concernant l'avant-projet de loi et le projet d'arrêté royal en matière de rétention de données (ci-après "l'avant-projet de loi et le projet d'arrêté royal"), et le projet d'arrêté royal relatif à l'obligation de collaboration (ci-après "le deuxième projet d'arrêté royal").

2. L'urgence est suffisamment motivée. La Commission émet dès lors ci-après un avis urgent concernant les projets précités, en tenant compte des informations dont elle dispose.

B. LÉGISLATION APPLICABLE

3. L'on peut tout d'abord se référer à la Directive 2006/24/CE. Étant donné que des données à caractère personnel sont traitées, la LVP est d'application, de même que la loi du 13 juin 2005 *relative aux communications électroniques* (ci-après la "LCE"). Il faut enfin 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. Le 2 juillet 2008, la Commission a déjà rendu un avis (n° 24/2008) *relatif à l'avant-projet de loi modifiant l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques et au projet d'arrêté royal fixant les données à conserver en application de l'article 126 de la loi du 13 juin 2005, ainsi que les conditions et la durée de conservation de ces données*. Son avis était à l'époque défavorable. C'est pourquoi le Ministre de la Justice soumet à présent à la Commission l'avant-projet de loi et le projet d'arrêté royal adaptés.

5. Le 3 septembre 2008, la Commission a émis l'avis n° 29/2008 *relatif au projet d'arrêté royal déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques*. Cet avis était également défavorable. Le deuxième projet d'arrêté royal est donc également soumis à présent à la Commission.

D. EXAMEN DE LA DEMANDE D'AVIS

6. La Commission examine ci-après dans quelle mesure ses remarques, telles que formulées dans les conclusions des avis précités, ont été respectées par les projets en question. Par commodité, l'ordre des remarques des avis a été maintenu ci-après, en mentionnant pour chaque point les modifications éventuellement apportées par le demandeur.

D.1. AVANT-PROJET DE LOI ET PROJET D'ARRÊTÉ ROYAL EN MATIÈRE DE RÉTENTION DE DONNÉES

7. *- (Avis n° 24/2008) - 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.*

8. En ce qui concerne la *durée de conservation*, aucune modification n'a été apportée dans l'avant-projet de loi : la durée de conservation ne peut pas être inférieure à 6 mois et ne peut dépasser 24 mois. Il appartient au Roi de fixer la durée de conservation exacte. La Commission maintient son point de vue selon lequel la durée de conservation exacte doit être fixée dans l'avant-projet de loi, vu l'importance de la matière. En ce qui concerne la durée de conservation, elle estime qu'une durée de 12 mois devrait suffire, cf. ci-après aux points 19 à 22 inclus. Il faudrait également stipuler dans l'avant-projet de loi que les données conservées doivent être détruites immédiatement au terme de ce délai.

9. L'Exposé des motifs mentionne toutefois une modification importante au commentaire de l'article 3 de l'avant-projet de loi. Celle-ci consiste à ce que deux ans après l'entrée en vigueur de cet arrêté royal, une évaluation de son application devra être réalisée, afin de pouvoir faire le point sur la nécessité et/ou la suffisance des délais impartis pour les besoins des autorités judiciaires. Le bénéfice de cette disposition réside dans le fait que l'on prévoit la possibilité d'adapter le délai de conservation, le cas échéant à la baisse, s'il ne correspondait plus à la réalité. Comme exposé ci-dessus, la Commission estime que la durée de conservation doit être fixée dans la loi. Il faudrait également inscrire dans la loi même, et non uniquement dans l'Exposé des motifs, qu'une évaluation aura lieu, et de quelle manière. D'après la Commission, cette évaluation devrait être double : *d'une part*, une grande évaluation unique, qui se ferait idéalement après l'évaluation européenne de la Directive 2006/24 qui est prévue, lors de laquelle on devrait fixer définitivement les critères ainsi que la durée de conservation. À titre d'exemple, on peut se référer à cet égard à la loi relative à l'institution et à l'organisation de la plate-forme eHealth, plus particulièrement à l'article 36,

qui fait mention d'une évaluation après deux ans. *D'autre part*, on devrait prévoir un rapport annuel au Parlement par le ministre responsable, par analogie avec ce que stipule l'article 90*decies* du Code d'instruction criminelle. Le rapport annuel en matière de rétention de données peut éventuellement être repris dans le rapport précité, conformément à l'article 90*decies* du Code d'instruction criminelle. La Commission suivra de près l'évaluation et le rapport susmentionnés.

10. Les *données à conserver* sont à présent définies comme suit dans l'avant-projet de loi (article 3, § 1) : "… *les opérateurs fournissant un service de téléphonie fixe accessible au public, un service de téléphonie mobile accessible au public, un service d'accès à l'Internet, un service de courrier électronique ou un service de téléphonie par Internet, 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 respective de réseaux ou de services de communications électroniques* …". Conformément à l'Exposé des motifs (partie générale, alinéas 3 et 4), la Directive 2006/24/CE établit la liste des données à conserver, subdivisée en catégories : identification de l'origine d'une communication, identification de la destination d'une communication, détermination des caractéristiques temporelles d'une communication, détermination du type de communication, ainsi que du matériel utilisé, et localisation du matériel utilisé. L'avant-projet de loi regroupe ces catégories de données sous les intitulés "données de trafic et de localisation" et "données d'identification d'utilisateurs finals". Ceux-ci sont ensuite développés davantage dans le projet d'arrêté royal. Les articles 88*bis* et 46*bis* du Code d'instruction criminelle et la terminologie de la LCE sont ainsi respectés. Par ailleurs, l'Exposé des motifs mentionne que la Directive crée également plusieurs sous-catégories au sein de ces différentes catégories de données, selon la nature des réseaux et services impliqués dans une communication : téléphonie fixe, téléphonie mobile, téléphonie par Internet, accès à l'Internet, et courrier électronique par Internet. Ces catégories sont également énumérées explicitement dans le projet d'article 126, de sorte que l'on sait clairement quels opérateurs sont soumis à l'obligation de conservation des données précitées.

11. L'Exposé des motifs stipule enfin (trois derniers alinéas de la partie générale) que la Directive 2006/24/CE établit le cadre général de la conservation des données relative aux communications électroniques. Seules quatre catégories de services de communications électroniques sont visées : la téléphonie fixe, la téléphonie mobile, l'accès à l'Internet et la messagerie électronique et la téléphonie via l'Internet. La technologie de la communication et les protocoles techniques qui règlent cette communication électronique se développent rapidement, en particulier en ce qui concerne les formes de la téléphonie via l'Internet. Pour que le cadre légal soit un instrument efficace dans la lutte contre la criminalité, il est

nécessaire que ce cadre puisse suivre l'évolution de ces protocoles techniques. Un arrêté royal permet une mise à jour rapide du cadre légal.

12. La Commission constate que dans l'avant-projet de loi, les catégories de données à conserver sont définies plus clairement. Leur élaboration via un arrêté royal peut être suivie, en tenant compte du fait que l'effet de l'avant-projet de loi et du projet d'arrêté royal sera évalué (cf. ci-avant, point 9), et qu'une éventuelle modification de l'arrêté royal doit être fixée après une concertation en Conseil des ministres, et ce après avis de la Commission et de l'Institut.

13. *- (Avis n° 24/2008) - 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.*

14. Le Rapport au Roi du projet d'arrêté royal mentionne que le cadre minimum fixé par la directive pour la conservation des données en matière de communications électroniques ne répond pas nécessairement aux besoins des services de police et des autorités judiciaires dans leurs missions de recherche, de détection et de poursuite d'infractions pénales. Ainsi, 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 — manquent à la liste établie par la directive. Le commentaire des articles du Rapport au Roi précise ensuite, par catégorie de données, quelles données doivent être conservées complémentairement, et pourquoi. Le demandeur a encore fourni des informations complémentaires à ce sujet à la Commission. Sur la base des données précitées, la Commission estime pouvoir conclure au caractère justifié du traitement envisagé, ce toutefois à condition qu'une évaluation ait lieu prochainement (cf. ci-dessus), la nécessité du traitement de ces données devant de nouveau être évaluée.

15. *- (Avis n° 24/2008) - 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.*

16. Dans sa version modifiée, l'avant-projet de loi prévoit à l'article 3, § 1, a) "la recherche, la détection et la poursuite d'infractions pénales *visées aux articles 46bis et 88bis du Code d'Instruction criminelle*". Le demandeur a précisé à la Commission que sa remarque avait été prise en compte grâce à cet ajout. L'article 46*bis* prévoit notamment la réclamation par le procureur du Roi de données d'identification relatives aux services de télécommunication,

l'article 88*bis* prévoit le repérage et la localisation de communications par le juge d'instruction. C'est en vue de l'applicabilité pratique de ces articles que les données d'identification, données d'appels et données de localisation qui sont visées doivent être conservées. Les deux articles prévoient également des conditions telles que la subsidiarité et la proportionnalité de la mesure. L'article 46*bis* est une compétence du procureur du Roi, l'article 88*bis* du juge d'instruction. Dans les deux cas, les mesures doivent être motivées par écrit et il y a donc des garanties que quiconque ne puisse pas accéder aux données conservées pour quelque raison ou infraction que ce soit. Les deux articles ne prévoient pas de liste des infractions mais un certain seuil est établi pour que ces articles limitent les mesures aux contraventions et crimes. Une énumération exhaustive des infractions graves n'est pas possible selon le demandeur, vu les diverses dispositions pénales particulières. En outre, une modification législative serait chaque fois nécessaire si une infraction devait être ajoutée.

17. La Commission peut être d'accord avec l'argumentation précitée, d'autant plus en raison de la précision apportée par le renvoi explicite aux articles 46*bis* et 88*bis* du Code d'instruction criminelle. L'article 46*bis* prévoit une motivation explicite par le procureur du Roi, laquelle doit refléter la proportionnalité en respectant la vie privée et la subsidiarité à l'égard de tout autre acte d'investigation. L'article 88*bis* prévoit une même disposition pour le juge d'instruction. Elle rappelle en outre que les données demandées par le magistrat qui ne sont pas utiles à l'enquête doivent être détruites.

18. *-(Avis n° 24/2008) - 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.*

19. Le projet d'arrêté royal a repris la durée de conservation de 24 mois du premier projet. Le Rapport au Roi stipule à ce sujet que sur la base de la pratique observée auprès des différents services de police décentralisés et auprès du Parquet fédéral en matière de demandes d'informations aux opérateurs et aux fournisseurs de réseaux ou de services de communications électroniques, ont peut considérer qu'un délai uniforme de 24 mois pour la conservation des différents types de données visés à l'article 126 de la loi constitue le mécanisme le plus approprié. Le demandeur a fourni à la Commission des exemples de situations dont il devrait ressortir qu'un délai de 24 mois est justifié, et que cela répond à un besoin réel de la police et de la justice.

20. Le demandeur a également informé la Commission d'une étude de l'IBPT relative aux délais de conservation à l'étranger, datant de juillet 2008. Il en ressort que différents pays (parmi lesquels l'Italie, la Slovénie, l'Irlande, le Portugal et les Pays-Bas) prévoient aussi un long délai (18 à 24 mois). D'autres pays (notamment la France, l'Allemagne et le Royaume-Uni) opteraient pour un délai plus court (12 mois). Selon le demandeur, cela serait davantage dicté par des raisons économiques et financières (frais pour les opérateurs).

21. La Commission a également pu prendre connaissance des points de vue de l'industrie des télécoms (ISPA). D'après les chiffres communiqués par cette dernière (étude d'octobre 2008), il apparaît que la durée prévue est, dans la plupart des pays (Danemark, France, Finlande, Espagne, Portugal), de 12 mois ; l'Allemagne a fixé une période de 6-7 mois. Dans d'autres pays, le délai proposé est souvent de 12 mois aussi (Royaume-Uni, Pays-Bas, Suède) ou de 6 mois (Autriche, Luxembourg). Elle fournit également des statistiques dont il devrait ressortir que la plupart des demandes de la justice adressées aux opérateurs de télécommunications belges ont lieu dans les six mois à compter du début de la conservation des données et que le nombre de demandes après 12 mois ne représente pas plus de 5 % du nombre total des demandes.

22. La Commission a pris note des arguments précités. Du point de vue de la justice, il est évident qu'une durée de conservation de 24 mois est nécessaire. L'industrie souhaite par contre limiter autant que possible cette durée de conservation, ce pour diverses raisons. La Commission estime qu'il est important, dans cette discussion, d'observer la finalité initiale de la directive, qui consiste en *l'harmonisation* de la législation dans les États membres en ce qui concerne la conservation de données de télécommunications par les opérateurs. Dans cette optique, le délai de 24 mois semble en ce moment être exagéré, vu le délai de 12 mois ou moins qui est d'application dans nos pays voisins (France, Pays-Bas, Allemagne, Luxembourg). La Commission estime dès lors qu'un délai de conservation de 12 mois est momentanément suffisant. Dans cette optique, l'évaluation envisagée est également importante, le délai pouvant être revu vers le haut ou vers le bas, si nécessaire. L'avant-projet de loi devrait enfin prévoir explicitement qu'au terme de cette durée de conservation, les données doivent être détruites immédiatement par l'opérateur.

23. *-(Avis n° 24/2008) - 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.*

24. Dans la version actuelle de l'avant-projet de loi, il n'est plus question des fournisseurs et revendeurs prévus à l'article 9, §§ 5 et 6 de la LCE. La Commission avait insisté sur ce point dans son avis précédent étant donné que l'on doit par exemple entendre par fournisseurs et revendeurs le réseau interne d'un groupe d'entreprises. Ceux-ci ne sont toutefois pas visés par la Directive 2006/24/CE, qui, conformément à l'article 3, s'applique exclusivement aux fournisseurs de services de communication électronique publics ou d'un réseau de communication public pour la fourniture des services de communication en question. D'où la demande de la Commission de supprimer les fournisseurs et revendeurs.

25. Étant donné que l'article 3 de la Directive 2006/24 prévoit que la directive ne s'applique qu'aux fournisseurs de services publics de communications électroniques ou d'un réseau public de télécommunications lors de la fourniture du service de communication en question, l'article 3, § 1 de l'avant-projet de loi doit être adapté. Le mot 'public' ne doit pas uniquement être utilisé dans l'article précité pour un service de téléphonie fixe et un service de téléphonie mobile, mais aussi pour un service d'accès à Internet, un service d'e-mail et un service de téléphonie par Internet. Cela doit donc devenir : un service public d'accès à Internet, un service public d'e-mail et un service public de téléphonie par Internet

26. L'avant-projet de loi prévoit à l'article 2 une adaptation de la notion d'opérateur dans la LCE (article 2, 11°) : "toute personne soumise à l'obligation d'introduire une notification conformément à l'article 9." Version actuelle de l'article 2, 11° de la LCE : "toute personne ayant introduit une notification conformément à l'article 9". Cette version offre toutefois une possibilité d'échappatoire : les opérateurs qui ne font pas de notification ne seraient ainsi pas soumis à la réglementation en matière de rétention de données. D'où l'adaptation de la définition. La Commission n'a pas de remarque à ce sujet.

27. *-(Avis n° 24/2008) - 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.*

28. Dans sa version modifiée, l'avant-projet de loi prévoit à l'article 3, § 1, b) et c) : "*la répression d'appels malveillants vers les services d'urgence, visée à l'article 107 de cette loi*" et "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, visée à l'article 43bis, § 3, 7° de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques*". Le demandeur estime que les deux finalités doivent être maintenues en vertu de l'article 126 de la LCE. Toutefois,

compte tenu des remarques de la Commission et par analogie avec la modification apportée au point a), il a été précisé de quels articles de loi il s'agissait, offrant ainsi davantage de clarté quant à l'application de l'obligation de conservation et aux modalités d'accès aux données, dont on reparlera plus en détail ci-après au point 32.

29. *-(Avis n° 24/2008) - 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.*

30. La Directive permet dans certains cas de dépasser la durée de conservation maximale prévue (24 mois). Cette possibilité est prévue dans l'avant-projet de loi à l'article 3, § 2 : "(…) *dans les circonstances exceptionnelles comme visées à l'article 4, § 2, le Roi peut* (…) *fixer un délai de conservation des données supérieur à 24 mois*". Dans la version précédente du projet de loi, seule l'expression "circonstances exceptionnelles" était mentionnée, laquelle n'offrait pas suffisamment de sécurité juridique aux yeux de la Commission, était extrêmement vague et de ce fait susceptible d'une interprétation trop large. Pour répondre à cette préoccupation, le demandeur a prévu de se référer, dans une définition, à l'article 4, § 1 de la LCE : les circonstances exceptionnelles sont donc ici "*lorsque la sécurité publique, la santé publique, l'ordre public ou la défense du Royaume l'exigent*". La Commission prend note de cette définition et demande que le demandeur donne, dans l'Exposé des motifs, les exemples utiles de ce que l'on entend par là. Ces exemples devraient être suffisamment importants.

31. *-(Avis n° 24/2008) - 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.*

32. Comme indiqué ci-dessus aux points 13 et 19, le renvoi explicite aux dispositions légales pertinentes dans l'avant-projet de loi (par exemple les articles 46*bis* et 88*bis* du Code pénal et l'article 107 de la LCE) doit fournir plus de clarté selon le demandeur, notamment en matière d'accès. Ainsi, l'article 46*bis* du Code pénal prévoit, d'après le demandeur, une compétence du procureur du Roi et l'article 88*bis* du Code d'instruction criminelle la compétence du juge d'instruction. Dans les deux cas, les mesures doivent être motivées par écrit et il y a donc des garanties que quiconque ne puisse pas accéder aux données conservées pour quelque raison ou infraction que ce soit.

33. *-(Avis n° 24/2008) - le non-respect des exigences en matière d'accès et d'utilisation des données collectées doit être sanctionné.*

34. Suite à sa remarque précédente (désigner explicitement qui a accès à quelles données), la Commission a demandé de criminaliser le non-respect des exigences d'accès et d'utilisation. Le demandeur y a satisfait, étant donné que l'avant-projet de loi prévoit désormais ce qui suit à l'article 4 : "*Est puni d'une amende de 50 à 50 000 EUR et d'une peine d'emprisonnement de quinze jours à deux ans ou d'une de ces peines seulement la personne qui, sachant qu'elle n'y est pas autorisée, accède aux données visées à l'article 126 ou fait usage des données à des fins autres que celles prévues dans cet article".* Cette criminalisation supplémentaire vise plus particulièrement à criminaliser l'utilisation des données conservées pour une finalité autre que celle prévue légalement. Ainsi, d'après l'Exposé des motifs, les autorités judiciaires peuvent également contrôler le bon déroulement de la conservation des données. La Commission recommande d'adapter le texte comme suit afin d'éviter les malentendus : "(…) *sachant qu'elle n'y est pas autorisée, accède aux données visées à l'article 126 ou,* ***si elle est autorisée à y accéder****, fait usage des données à des fins autres que celles prévues à* ***l'article 126****".*

D.2. LE PROJET D'ARRÊTÉ ROYAL RELATIF À L'OBLIGATION DE COLLABORATION

35. *- (Avis n° 29/2008) le projet d'arrêté royal fixant les données à conserver en application de l'article 126 LCE, ainsi que les conditions et la durée de conservation de ces données (arrêté royal "conservation"), pour lequel la Commission a émis un avis défavorable, est intimement lié au projet d'Arrêté Royal déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques (arrêté royal "collaboration") ;*

36. À ce sujet, le demandeur a communiqué à la Commission que si le lien étroit entre les deux arrêtés royaux était clair, il n'était quand même pas recommandé de régler les deux matières dans un seul texte. Avant tout, les deux textes ont une base légale différente (LCE et Code d'instruction criminelle). Le demandeur souligne également que l'obligation de conservation des données et l'obligation de collaboration ne se chevauchent pas forcément intégralement (différence du concept "opérateur" dans la LCE et le Code d'instruction criminelle). L'obligation de collaboration est plus large. Par ailleurs, l'obligation de collaboration est déjà régie dans l'arrêté royal du 9 janvier 2003, qui est abrogé par le deuxième projet d'arrêté royal.

37. *-(Avis n° 29/2008) les mêmes défauts, pointés dans l'avis 24/2008, entachent l'arrêté royal "collaboration", à savoir l'application des règles de collaboration aux fournisseurs et revendeurs visés à l'article 9, §§ 5 et 6 LCE, ainsi que l'absence d'une sanction attachée au non-respect des exigences en matière d'accès et d'utilisation des données ;*

38. Dans le deuxième projet d'arrêté royal, la définition du secteur Internet est maintenue. Conformément au Rapport au Roi, il faut tenir compte, en ce qui concerne cette définition, de l'article 2 de la LCE, qui définit les notions de "point de terminaison du réseau", "utilisateur", "utilisateur final" et "service de communications électroniques". L'on a tenté de suivre autant que possible la terminologie de cette loi. En principe, il faut entendre par là tous les niveaux du secteur Internet : les opérateurs qui mettent leur infrastructure à disposition pour le transport des signaux Internet (connexion physique), les fournisseurs d'accès à Internet qui donnent accès à Internet à l'utilisateur final et les fournisseurs de services Internet qui offrent sur Internet des services de communication. Le demandeur a pu confirmer à la Commission que l'on n'entendait pas par là les fournisseurs et revendeurs prévus à l'article 9, §§ 5 et 6 de la LCE. Un règlement distinct sera prévu pour ces derniers.

39. Dans son avis, la Commission avait proposé de souligner dans le texte de l'article 2, § 2, premier alinéa du projet d'arrêté royal que les membres du personnel et les préposés des opérateurs, en vertu des articles 46*bis*, § 2, troisième alinéa, 88*bis*, § 2, deuxième alinéa et 90*quater*, deuxième alinéa du Code d'instruction criminelle, devaient respecter le secret professionnel conformément à l'article 458 du Code pénal. Le Rapport au Roi relatif au deuxième projet d'arrêté royal mentionne ce qui suit dans le commentaire de l'article 2 : "*Il est extrêmement important que les membres du personnel de la Cellule de coordination soient fiables. Ils doivent en effet traiter des informations sensibles. C'est important également dès lors que l'article 90quater, § 2, alinéa 2, du Code d'instruction criminelle prévoit des sanctions pénales en cas de violation de l'obligation de secret, conformément à l'article 458 du Code pénal*." La Commission recommande de se référer également dans ce cadre aux articles 46*bis* et 88*bis* du Code d'instruction criminelle.

40. *-(Avis n° 29/2008) le service NTSU-CTIF, désigné pour accéder directement à ces bases de données, doit être, vu le principe de légalité, plus clairement défini ;*

41. L'article 1er du deuxième projet d'arrêté royal définit le service NTSU-CTIF : le système central d'interception technique du service de police intégrée, structuré à deux niveaux. Le demandeur a notamment transmis à la Commission un organigramme afin de mieux comprendre ce service. Selon la Commission, il est recommandé de rendre ces informations

publiques, de sorte que quiconque puisse retrouver ce service au sein des services de la police fédérale.

42. *-(Avis n° 29/2008) le changement de pratique, à savoir l'accès direct, par un service de police, aux bases de données "clients" des opérateurs télécom doit être davantage justifié, et si elle s'impose, cette pratique devrait être entourée de garanties (règles d'accès, log, journalisation des accès et consultations, accès authentifié,…) dans le corps du texte du projet d'arrêté royal ;*

43. Le deuxième projet d'arrêté royal fait une distinction entre d'une part les opérateurs à qui une capacité de numérotation a été attribuée dans le plan national de numérotation et d'autre part les autres opérateurs. Ce n'est que dans le premier cas que les opérateurs sont tenus d'accorder au service NTSU-CTIF un accès à la banque de données contenant le fichier clients. Conformément à l'article 3, cet accès sera implémenté par une application Internet sécurisée, sur la base d'une requête électronique à laquelle l'opérateur sera tenu de répondre de manière automatique. Le service NTSU-CTIF fixe les détails techniques complémentaires de cette procédure. Le service NTSU-CTIF conserve un log et fait un journal de chaque accès et consultation de la banque de données. Conformément au Rapport au Roi, cela ne signifie pas pour autant que le service NTSU-CTIF pourra consulter sans condition cette base de données à n'importe quel moment. Il y a lieu bien entendu d'observer les règles du Code d'instruction criminelle et ce n'est qu'à la réception de la requête visée à l'article 466*bis* par le service NTSU-CTIF qu'il pourra consulter la base de données. Les opérateurs peuvent par ailleurs voir quand ce service accède aux fichiers des clients et dénoncer l'accès qui ne s'effectue pas sur la base de la procédure décrite dans l'arrêté royal : une requête électronique du service NTSU-CTIF est requise.

44. D'après le demandeur, le but était que le NTSU/CTIF puisse consulter plus facilement un fichier reprenant les données des clients des opérateurs, ce en particulier grâce à une requête traitée électroniquement par le NTSU/CTIF (et plus des consultations manuelles ou téléphoniques et encore moins par fax). L'automatisation des processus accroît la rapidité avec laquelle les informations sont mises à disposition des demandeurs, réduit la charge de travail manuel et les risques d'erreurs lors du traitement (faute de frappe par exemple) et permet le contrôle a posteriori de toutes les requêtes introduites (en particulier grâce à un logging). Toujours d'après le demandeur, ce processus automatisé est plus respectueux de la vie privée que les consultations manuelles, téléphoniques ou par fax, qui ne permettent pas par exemple le contrôle via des loggings, et n'empêchent pas le risque de perte de données et les éventuelles fautes lors du traitement de données. Il est également important que seules les requêtes passent via le NTSU/CTIF et y soient contrôlées. Les réponses sont

par contre transmises directement au demandeur initial sans passer de nouveau par le NTSU/CTIF. C'est également favorable à la protection de la vie privée. D'après le demandeur, le NTSU prend deux types de mesures pour protéger les données relatives aux mesures pour lesquelles il est responsable :

- mesures physiques : accès limité, accès contrôlé par un badge, bâtiment protégé physiquement, occupation permanente, caméras, logging des personnes qui entrent et sortent ;

- mesures logicielles : octroi de droits sur la base de profils spécifiques, contrôle de logging de chaque acte posé sur le réseau, accès octroyé par dossier (pas d'accès général) lorsque le nom de la personne concernée est mentionné spécifiquement sur le réquisitoire du juge d'instruction, transfert sécurisé.

45. La Commission propose d'ajouter le passage suivant à l'article 3, premier alinéa du deuxième projet d'arrêté royal : "(…) Le service NTSU-CTIF conserve un log et fait un journal de chaque accès et consultation de la banque de données. *Il prend également les mesures physiques et logicielles nécessaires pour prévoir un niveau de protection adéquat.*"

46. *-(Avis n° 29/2008) le principe de proportionnalité n'est pas respecté en ce qui concerne la transmission des coordonnées personnelles des membres des Cellules Coordination de la Justice.*

47. Le deuxième projet d'arrêté royal prévoit à l'article 2, § 3 qu'un gsm de service est mis à la disposition de la Cellule de coordination. Il a ainsi été satisfait à la remarque formulée par la Commission dans son avis, et la mise à disposition des données privées des membres de la cellule a été supprimée.

PAR CES MOTIFS,

la Commission émet un avis *favorable*, uniquement à la condition qu'il soit tenu compte des remarques formulées concernant :

- la détermination de la durée de conservation de 12 mois dans l'avant-projet de loi (point 8) ;
- l'évaluation parlementaire de l'avant-projet de loi et du projet d'arrêté royal ainsi que le rapport annuel au parlement par le ministre compétent (point 9) ;
- la durée de conservation de 12 mois et la destruction immédiate des données conservées au terme de ce délai (points 19 à 22 inclus) ;
- l'utilisation du terme 'public' pour un service d'accès à Internet, un service d'e-mail et un service de téléphonie par Internet (point 25) ;
- la définition de la notion de 'circonstances exceptionnelles' (point 30) ;

- l'incrimination des exigences d'accès et d'utilisation (point 34) ;
- le service NTSU-CTIF (points 41-45).

Pour l'Administrateur e.c.,

(sé) Patrick Van Wouwe

Le Président,

(sé) Willem Debeuckelaere