Avis n° 24/2010 du 30 juin 2010

Objet: Projet d'arrêté royal portant exécution de diverses dispositions de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (CO/A/2010/022)

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

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

Vu la demande d'avis de Monsieur Stefaan De Clerck, Ministre de la Justice, reçue le 31/05/2010 ;

Vu le rapport de Monsieur Frank Schuermans ;

Émet, le 30 juin 2010, l'avis suivant :

A. Introduction

1. Le 31 mai 2010, le Ministre de la Justice a demandé à la Commission d'émettre un avis concernant un projet d'arrêté royal portant exécution de diverses dispositions de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

2. Vu l'adoption de la loi du 4 février 2010 *relative aux méthodes de recueil des données par les services de renseignement et de sécurité*, plusieurs habilitations ont été laissées au Roi afin de prendre des mesures d'exécution des nouvelles dispositions modifiées de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

B. Analyse du projet d'arrêté royal

3. Dans les visas, il serait opportun de libeller de la manière suivante : "vu l'avis de la Commission de la protection de la vie privée, donné le 30 juin 2010". En effet, l'examen de la Commission ne s'est pas limité aux seuls articles 12, 13 et 14 mais a porté sur l'entièreté du projet d'arrêté royal.

Utilisation d'un faux nom
(article 13/1 de la loi du 30 novembre 1998 ~ article 2 du projet d'AR).
4. Le dirigeant du service de renseignement et de sécurité tient à jour un journal de bord spécifique dans lequel on trouvera :
- la liste des faux noms utilisés et le lien avec l'agent qui les utilise ;
- les dates, contexte et, le cas échéant, les incidents survenus concernant l'utilisation du faux nom.

Accès aux banques de données publiques
(article 14, alinéa 4 de la loi du 30 novembre 1998 ~ article 3 du projet d'AR).
5. Si le service de renseignement et de sécurité a un accès direct à la banque de données :
- une liste nominative des personnes habilitées à accéder est tenue en permanence à la disposition de la Commission ;
- un fichier log (c'est-à-dire une journalisation des accès à la banque de données) est généré à chaque demande de consultation. Il est conservé 12 mois au minimum.

6. L'article 14, 4ème alinéa de la loi organique passe sous silence le fait de savoir si l'accès aux banques de données du secteur public peut également se faire de manière secrète. Par conséquent, la question se pose de savoir s'il n'est pas opportun d'informer en principe le gestionnaire de la banque de données de la consultation chaque fois qu'une telle consultation est effectuée par les services de renseignement afin de respecter le principe de transparence. Une notification en ce sens semble en effet nécessaire. Seule une motivation solide pourrait permettre une dérogation à ce

principe, le cas échéant, après avis de la commission administrative, étant donné qu'une consultation secrète de la banque de données d'autrui ne semble pas évidente. Les mesures nécessaires doivent en effet être prises afin qu'une telle notification ne compromette pas le caractère secret du travail de renseignement, ce qui serait par exemple possible en n'avertissant qu'une ou quelques personnes et en prenant d'autres mesures techniques. Cette remarque est d'autant moins logique que dans le cas où aucun accès direct n'est prévu, l'agent du service de renseignement doit présenter sa carte de légitimation au gestionnaire de la banque de données (cf. le point 7). Le délai prévu de 12 mois semble toutefois être un minimum. La Commission recommande de conserver les données de journalisation pendant 10 ans, *a fortiori* lorsqu'il s'agit de consultations secrètes d'autres bases de données.
Ce délai de 10 ans est comparable à celui appliqué habituellement dans le secteur social et imposé par la section Sécurité sociale du Comité sectoriel de la Sécurité sociale et de la Santé. Du point de vue de l'investissement, cela ne représente qu'un petit effort supplémentaire et ce délai permet de pouvoir détecter, avec bien plus de certitude, des abus lors d'une inspection ou d'un contrôle ultérieur.

7. Si le service de renseignement et de sécurité n'a pas d'accès direct à la banque de données, les données sont communiquées immédiatement à l'agent du service de renseignement et de sécurité, sur présentation de sa carte de légitimation.
La Commission recommande qu'à l'instar de ce qui est prévu pour l'accès direct, une journalisation des demandes soit enregistrée par le gestionnaire de la base de données et qu'une trace écrite de cette consultation apparaisse également au niveau du service de renseignement et de sécurité. Ces consultations doivent naturellement également faire l'objet d'une journalisation.

8. Un conseiller à la sécurité est désigné au sein de chaque service de renseignement et de sécurité : il est chargé de garantir le respect de la loi lors de toute demande de données et de prendre toutes les mesures utiles afin d'assurer la sécurité des informations enregistrées (article 4 du projet d'AR).
La Commission insiste également sur l'importance de la position indépendante que le préposé à la protection des données ou le conseiller en sécurité doit avoir au sein de l'organisation. Il ne doit rendre des comptes et faire rapport qu'au chef du renseignement – ou du service de sécurité (à savoir l'administrateur général de la Sûreté de l'État ou le Chef du Service Général du Renseignement et de la Sécurité). Il doit aussi avoir la possibilité, sans crainte de sanctions ou d'autres conséquences négatives, de faire rapport directement à la commission administrative et cette dernière ou le Comité R doit pouvoir interroger directement l'intéressé. Enfin, il importe que l'intéressé jouisse d'une certaine protection statutaire comme c'est par exemple le cas pour les membres de l'organe de contrôle des informations policières (cf. article 44/7, dernier alinéa de la loi du 5 août 1992 *sur la fonction de police*) de manière à pouvoir remplir sa fonction en toute

indépendance. La Commission note qu'une terminologie différente est employée (tant en français qu'en néerlandais), au risque de créer éventuellement une divergence d'interprétation : le projet d'arrêté royal institue un "conseiller à la sécurité des données". La Commission recommande plutôt d'aligner le libellé de l'article 4 du projet d'arrêté royal sur la terminologie existante : soit en se basant sur l'article 17*bis* de la LVP (préposé à la protection des données) ; soit en se basant sur l'article 10 de la loi du 8 aout 1983 *organisant un registre national des personnes physiques* (conseiller en sécurité de l'information).

9. Quelle que soit la dénomination finalement retenue par les auteurs du projet d'arrêté royal, ce "conseiller à la sécurité" remplira aussi de facto la fonction de "préposé à la protection des données" au sens de l'article 17*bis* de la LVP.

Identité et la qualité fictive

(article 18/13 de la loi du 30 novembre 1998 ~ article 6 du projet d'AR).

10. Le dirigeant du service de renseignement et de sécurité tient à jour un journal de bord spécifique dans lequel on trouvera :

- la liste des identités et qualités fictives utilisées et le lien avec l'agent qui les utilise ;
- les dates, contexte et, le cas échéant, les incidents survenus concernant l'utilisation de ces identités et qualités fictives.

La Commission aimerait également que le journal de bord soit conservé au moins 10 ans après que l'identité et la qualité fictive ne soit plus active (cf. point 6).

Destruction des enregistrements des communications

(article 18/17 de la loi du 30 novembre 1998 ~ article 7 du projet d'AR).

11. La destruction sera opérée au moyen des procédés techniques les plus appropriés compte tenu de l'évolution de la technologie en la matière, de sorte qu'il ne soit plus possible d'exploiter les données.

Rétribution de la collaboration avec les services de renseignements

(article 18/18 de la loi du 30 novembre 1998 ~ article 8 du projet d'AR).

12. Ces dispositions n'appellent pas de remarque.

Contrôle des méthodes spécifiques et exceptionnelles

(articles 43/1 et 18/10 de la loi du 30 novembre 1998 ~ article 9 du projet d'AR).

13. Une Commission indépendante administrative *ad hoc* est chargée par la loi de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données par les services de renseignement et de sécurité (article 43/1).

14. Cette Commission est régulièrement informée (par voie électronique sécurisée) du déroulement des méthodes exceptionnelles (article 9, alinéa 1er du projet d'AR). En outre, toute décision ou autorisation – et de manière générale tout document – échangé entre cette Commission et le service de renseignement et de sécurité s'effectue dans le respect des règles et directives concernant le transfert d'informations classifiées en vertu de la loi du 11 décembre 1998 (article 11, alinéa 6 du projet d'AR).

15. Les données recueillies dans des conditions qui ne respectent pas les dispositions légales en vigueur sont placées sous scellé, sans délai, en vue de leur conservation, dans un lieu sécurisé désigné par la Commission (visée à l'article 43/3). En attendant la décision du Comité R (conformément à l'article 43/6, § 1er de la loi du 30 novembre 1998), les données sous forme électronique sont rendues illisibles de sorte qu'il ne soit plus possible de les exploiter (article 12 du projet d'AR).

16. La destruction de ces données illégalement recueillies s'effectue sous le contrôle de la Commission (visée à l'article 43/3) et au moyen des procédés techniques les plus appropriés compte tenu de l'évolution de la technologie en la matière, de sorte qu'il ne soit plus possible d'exploiter les données. Un rapport de destruction est rédigé à cet effet (article 13 du projet d'AR).

17. la Commission recommande un meilleur libellé de l'article 12 du projet d'AR : les données "papier" sont conservées de manière sécurisée sans possibilité d'accès. Il devrait en être de même pour les données électroniques.
Il faut également prévoir que ces données puissent être décryptées (rendues à nouveau lisibles) si le Comité R adopte une décision favorable concernant la méthode utilisée.

Compétence du Comité R et de la CPVP
(article 14 du projet d'AR).
18. Dans le cadre d'examen de dossiers sur base de l'article 13 de la LVP (accès indirect aux traitements de données générés par les services de police ou par les services de renseignement et de sécurité), la Commission peut s'adresser au Comité R selon la procédure suivante :
- une demande motivée (et transmise selon les règles de transfert d'informations classifiées) ;
- étayée par une suspicion raisonnable ;
- que des données à caractère personnel sont recueillies via une méthode spécifique ou exceptionnelle ;
- et au mépris de la loi du 30 novembre 1998.

19. La Commission pourra donc, dans le cadre d'examen de dossiers sur base de l'article 13 de la LVP, effectuer en toute connaissance de cause, les vérifications nécessaires.

20. La Commission note que l'accès aux données recueillies *a priori* légalement reste toujours possible, sans procédure particulière, par une demande au service de renseignement et de sécurité concerné (article 32 de la LVP).

PAR CES MOTIFS,

Vu les remarques formulées dans le présent avis, la Commission de la protection de la vie privée émet, moyennant le respect de ses observations aux points 3, 6, 7 et 17 du présent avis, un avis **favorable** quant au contenu actuel du projet d'arrêté royal.

Pour l'Administrateur e.c., Le Président,

(sé) Patrick Van Wouwe (sé) Willem Debeuckelaere