



AVIS N° 04 /2005 du 14 mars 2005.

N. Réf. : SA2 / A / 2005 / 002

OBJET : Projet d'arrêté royal modifiant l'arrêté royal du 9 juillet 2001 réglementant la destruction des banques de données de la Banque-carrefour de la Sécurité Sociale et des banques de données sociales ou des données sociales à caractère personnel y conservées, en exécution de l'article 29 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la Sécurité Sociale.

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, en particulier l'article 29 ;

Vu la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la Sécurité Sociale, en particulier l'article 29 ;

Vu la demande d'avis du 24 janvier 2005 émanant du Ministre des Affaires Sociales et de la Santé publique ;

Vu le rapport de Madame F. D'Hautcourt ;

Emet, le 14 mars 2005, l'avis suivant :

I. OBJET DE LA DEMANDE D'AVIS.

Le projet d'arrêté royal que le Ministre des Affaires sociales et de la Santé publique soumet à la Commission concerne la modification d'un certain nombre de dispositions de l'arrêté royal du 9 juillet 2001 réglementant la destruction des banques de données de la Banque-carrefour de la Sécurité sociale et des banques de données sociales ou des données sociales à caractère personnel y conservées, en exécution de l'article 29 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la Sécurité Sociale.

L'idée d'une telle modification vient de la constatation que l'application de l'arrêté royal susmentionné du 9 juillet 2001 engendre, dans sa forme actuelle, des problèmes dans la pratique, puisque l'accent est mis sur une stratégie de destruction, plutôt que sur une stratégie de renforcement permanent de la protection et de la sécurité des systèmes d'information de la sécurité sociale.

Le présent projet d'arrêté royal a pour but d'y remédier en remplaçant d'une part la procédure de destruction existante par une procédure adaptée aux circonstances et en supprimant d'autre part, pour les personnes chargées de la gestion journalière de la Banque-carrefour de la Sécurité Sociale et des institutions de sécurité sociale, l'obligation de rédiger un manuel à ce sujet.

II. CADRE LEGAL.

Outre la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, la disposition légale suivante constitue l'objet de la demande d'avis :

L'article 29 de la loi du 15 janvier 1990 relative à l'institution et à l'organisation d'une Banque-carrefour de la Sécurité Sociale stipule que « Le Roi désigne, par arrêté délibéré en Conseil des Ministres, les personnes qui, en cas de guerre, dans des circonstances y assimilées en vertu de l'article 7 de la loi du 12 mai 1927 sur les réquisitions militaires ou pendant l'occupation du territoire national par l'ennemi, sont chargées de détruire ou de faire détruire les banques de données de la Banque-carrefour et les banques de données sociales ou les données sociales à caractère personnel y conservées. Le Roi fixe les conditions et les modalités d'une telle destruction, en veillant à ne pas compromettre, autant que possible, l'application de la sécurité sociale ».

Concrètement, le projet d'arrêté royal tend à :

- adapter les articles 2, 3 et 5 de l'arrêté royal du 9 juillet 2001 dans le sens où la procédure à appliquer en cas de guerre, dans des circonstances y assimilées en vertu de l'article 7 de la loi du 12 mai 1927 sur les réquisitions militaires ou pendant l'occupation du territoire national par l'ennemi, ne doit pas nécessairement conduire à une destruction des banques de données sociales ou des données sociales à caractère personnel y conservées ;
- abroger l'article 6 de l'arrêté royal du 9 juillet 2001 qui stipule que les personnes chargées de la gestion journalière de la Banque Carrefour de la Sécurité Sociale et des institutions de sécurité sociale doivent rédiger un manuel interne relatif à la problématique de la destruction des banques de données sociales en cas de guerre et dans des circonstances y assimilées.

III. EXAMEN DE LA DEMANDE D'AVIS.

1. La Commission souhaite au préalable faire remarquer qu'en ce qui concerne certains éléments du présent projet d'arrêté, on se trouve à la frontière entre la compétence du Conseil d'Etat d'une part et de la Commission d'autre part. Ce n'est pas nouveau. Cette constatation a déjà été faite par le passé.

Toutefois, vu que le projet d'arrêté a pour objet le traitement de données à caractère personnel, plus particulièrement le renforcement de leur sécurité avant de procéder à leur destruction, et les éventuelles conséquences sur la protection de la vie privée des personnes auxquelles se rapportent les données, la Commission juge que cela fait partie de ses missions de se prononcer à ce sujet.

2. La Commission constate que le présent projet d'arrêté royal a déjà été soumis au Comité de gestion de la Banque-carrefour de la Sécurité Sociale qui a rendu un avis favorable sur cet arrêté royal lors de sa séance du 23 mars 2004.

3. La finalité de la modification prévue de l'arrêté royal du 9 juillet 2001 consiste à mettre l'accent sur l'aspect sécurité et l'augmentation inhérente y afférente du niveau de sécurité des systèmes d'information de la sécurité sociale plutôt que sur la destruction de ces banques de données au cas où surviendrait une guerre ou une situation y assimilée comportant un risque potentiel d'abus des données à caractère personnel qui y sont reprises.

La finalité ainsi poursuivie doit être considérée comme légitime au sens de l'article 4, § 1, 2° de la loi du 8 décembre 1992, d'autant plus que la rapide évolution de la technologie permet actuellement d'instaurer des mesures de sécurité accrues en vertu desquelles on ne devra recourir à cette mesure radicale qu'à un stade ultérieur d'absolue nécessité de destruction des données.

4. Une réflexion générale que la Commission émet concernant le règlement développé dans l'arrêté royal du 9 juillet 2001 et dans les modifications qui y sont apportées par le projet d'arrêté royal consiste à dire qu'à partir de considérations de sécurité, il serait souhaitable qu'une telle procédure ne reste pas purement limitée aux données à caractère personnel reprises dans les banques de données sociales, mais qu'elle soit étendue à d'autres fichiers de données.

Une généralisation du règlement prévu pour les données sociales serait possible sur la base de l'article 45 de la loi du 8 décembre 1992 qui stipule que « Le Roi peut déterminer les autorités qui donneront l'ordre de détruire ou qui seront chargées de la destruction des traitements des données en temps de guerre et pendant les époques qui lui sont assimilées en vertu de l'article 7 de la loi du 12 mai 1927 sur les réquisitions militaires, ainsi que pendant l'occupation du territoire belge par l'ennemi ». Toutefois, jusqu'à présent, cette disposition légale n'a jamais été mise à exécution.

5. Ci-dessous, un commentaire, article par article, concernant les modifications de l'arrêté royal du 9 juillet 2001 prévues par le présent projet d'arrêté :

- *Article 2 de l'arrêté royal du 9 juillet 2001, tel que modifié par l'article 1^{er} du projet d'arrêté.*

La modification de cette disposition par l'article 1^{er} du projet d'arrêté tend à ce que le Ministre compétent pour l'application de la sécurité sociale ne puisse plus soumettre à discussion, à la commission interdépartementale, la problématique mais uniquement la 'nécessité' de la destruction des banques de données ou des données sociales à caractère personnel y conservées.

Limiter la présentation à la commission interdépartementale à la nécessité de la destruction de ces banques de données constitue déjà une indication de la préoccupation concernant la garantie de la continuité de la sécurité sociale, avant que l'on ne procède à la destruction des banques de données sociales. Par conséquent, cette modification apportée par le projet d'arrêté est considérée comme une amélioration par la Commission.

- *Article 3, premier alinéa de l'arrêté royal du 9 juillet 2001, tel que modifié par l'article 2 du projet d'arrêté.*

La modification de l'article 3, premier alinéa, 1° dudit arrêté royal par l'article 2 du projet d'arrêté qui met l'accent sur le fait que la commission interdépartementale émet un avis motivé sur la création de *'minimum une copie du système d'information'* sur supports électroniques constitue une précision approuvée par la Commission.

Concernant l'adaptation apportée par le projet d'arrêté à l'article 3, premier alinéa, 2°, la Commission fait remarquer qu'il semble superflu d'ajouter *'selon un processus encore à préciser'* lorsqu'il est stipulé que la transmission des supports électroniques par la Banque-carrefour de la Sécurité Sociale et les institutions de sécurité sociale à une instance responsable de leur sécurité encore à préciser est soumise à l'avis motivé de la commission interdépartementale. La transmission des supports électroniques implique déjà en soi que cela doit se faire selon un processus déterminé, de sorte que l'ajout *'selon un processus encore à préciser'* n'apporte pas d'explication complémentaire.

L'adaptation de l'article 3, premier alinéa, 3° qui consiste à remplacer *'la destruction'* par *'la nécessité de la destruction, selon une méthode adaptée à l'urgence de la situation'* des banques de données dans lesquelles sont conservées des données sociales par ou pour le compte de la Banque-carrefour de la Sécurité Sociale et des institutions de sécurité sociale, est jugée positive par la Commission, en raison de la cohérence ainsi établie avec la modification susmentionnée de l'article 2 de l'AR du 9 juillet 2001 par l'article 1^{er} du projet d'arrêté.

Bien que l'article 3, deuxième et troisième alinéas de l'AR du 9 juillet 2001 restent inchangés, la Commission attire quand même l'attention sur le fait que pour les mêmes raisons, à savoir la cohérence avec les autres corrections déjà apportées par le projet d'arrêté, il serait judicieux de remplacer à l'article 3, troisième alinéa les termes *'la problématique de la destruction des banques de données'* par les termes *'la nécessité de la destruction des banques de données'*.

- *Article 5 de l'arrêté royal du 9 juillet 2001, tel que modifié par l'article 3 du projet d'arrêté.*

A l'exception du fait que l'énumération des missions dont sont responsables les personnes chargées de la gestion journalière de la Banque-carrefour et des institutions de sécurité sociale soit remplacée par la référence à la décision des Ministres réunis en Conseil concernant ces missions énumérées à l'article 3, premier alinéa, l'article 5 reste inchangé.

La Commission souhaite formuler une remarque concernant cette disposition. Selon elle, il est recommandé de désigner plus précisément la personne qui sera chargée d'exécuter la décision des ministres. Elle suggère qu'il s'agisse du conseiller en sécurité de la Banque-carrefour.

De plus, la Commission signale l'importance de conserver la dernière phrase de l'article 5, § 3, deuxième alinéa qui stipule que « En toute hypothèse, la destruction doit avoir pour conséquence l'inutilisabilité complète des données sociales à caractère personnel. ».

- Article 6 de l'arrêté royal du 9 juillet 2001, tel qu'abrogé par l'article 4 du projet d'arrêté.

L'actuel article 6 dit ceci : « Les personnes chargées de la gestion journalière de la Banque-Carrefour de la Sécurité Sociale et des institutions de sécurité sociale rédigent un manuel relatif aux obligations mentionnées à l'article 5, § 1^{er}.

Ce manuel comprend au moins les éléments suivants :

1° par banque de données sociales, une description précise des modes possibles selon lesquels les données sociales à caractère personnel y reprises peuvent être copiées sur supports électroniques ;

2° par banque de données sociales, une description précise des modes de destruction possibles ;

3° une description de la fonction de la personne qui exécutera la destruction des banques de données sociales ;

4° par banque de données sociales, une description précise des modes de reconstruction de la banque en temps de paix ;

5° si la gestion des banques de données sociales et des données sociales à caractère personnel est confiée à un sous-traitant, la manière selon laquelle la décision des Ministres réunis en Conseil visée à l'article 3, alinéa 2, sera exécutée.

Le manuel est rédigé dans un délai de 24 mois à compter du premier jour du mois de l'entrée en vigueur du présent arrêté.

Le Comité de Surveillance près la Banque-Carrefour de la Sécurité Sociale veille au respect de la présente disposition. »

Compte tenu des rapides progrès technologiques qui ont pour conséquence que la rédaction d'un tel manuel détaillé qui devrait notamment décrire les modes de destruction, n'est pratiquement pas réalisable, puisqu'il est impossible de l'actualiser de manière permanente et de l'adapter aux développements technologiques, la Commission estime qu'il n'y a aucune objection à l'abrogation de cette disposition, à condition de maintenir le principe selon lequel, dans des cas d'absolue nécessité, on procède à la destruction des données en question. Afin de conserver ce principe, il est conseillé d'ajouter une norme aux normes de sécurité existant au sein de la Banque-carrefour de la Sécurité Sociale, norme dans laquelle il serait précisé que le conseiller en sécurité de la Banque-carrefour est responsable de la surveillance de la protection et de la destruction des données. Le délai dans lequel la destruction doit avoir lieu doit également être indiqué.

La Commission fait en effet observer qu'au sein de la Banque-carrefour de la Sécurité Sociale, des normes minimales de sécurité ont déjà été élaborées. Celles-ci doivent être respectées par les institutions sociales afin que ces dernières puissent être connectées au réseau de la Banque-carrefour de la Sécurité Sociale et elles sont axées sur la garantie de la sécurité des données sociales à caractère personnel dans ses diverses formes.

Dans cet ensemble de règles formulées de manière générale, il a déjà été explicitement établi que toute institution de sécurité sociale qui est connectée au réseau doit prévoir un système de copies de sécurité à contrôler régulièrement (back up) afin d'éviter, en cas de catastrophe limitée ou totale, toute perte irréparable de données nécessaires à l'application et l'exécution de la sécurité sociale. En outre, il y a l'obligation d'élaborer, tester et observer un plan de continuité afin de pouvoir garantir les missions de l'institution en matière de sécurité sociale. Il faut également prévoir un centre informatique de secours en cas de catastrophe limitée ou totale.

Concernant ces normes, qui ont une valeur contraignante, il est expressément prévu que celles-ci sont susceptibles d'être revues et peuvent donc être adaptées en fonction de l'évolution qui se produit sur le plan légal, technique ou sur un autre plan.

Etant donné que c'est le comité sectoriel de la sécurité sociale qui veille au respect de l'ensemble des règles minimales de sécurité par les institutions sociales, la Commission estime que la rédaction d'un manuel, telle qu'elle est prescrite par l'article 6 de l'arrêté royal du 9 juillet 2001, n'est pas utile.

PAR CES MOTIFS,

La Commission émet un avis favorable concernant le présent projet d'arrêté royal, moyennant la prise en considération des remarques exposées ci-dessus.

L'administrateur,

Le président,

(sé) Jo BARET

(sé) Michel PARISSE