



**Comité sectoriel de la Sécurité sociale et de la Santé
Section « Sécurité sociale »**

SCSZ/09/042

DELIBERATION N° 09/030 DU 5 MAI 2009 RELATIVE A LA COMMUNICATION DE DONNEES A CARACTERE PERSONNEL PAR LA BANQUE CARREFOUR DE LA SECURITE SOCIALE AU SERVICE PUBLIC FEDERAL TECHNOLOGIE DE L'INFORMATION ET DE LA COMMUNICATION (FEDICT) EN VUE DU TEST, DE L'AMELIORATION, DE LA MAINTENANCE ET DU MONITORING DES APPLICATIONS INFORMATIQUES

Vu la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, notamment l'article 15, § 1^{er}, alinéa 2;

Vu la demande du service public fédéral Technologie de l'information et de la communication du 29 avril 2009;

Vu le rapport d'auditorat de la Banque Carrefour de la sécurité sociale du 29 avril 2009 ;

Vu le rapport de monsieur Yves Roger.

1. OBJET DE LA DEMANDE

- 1.1.** En vue de l'accomplissement de ses missions légales et réglementaires, le service public fédéral Technologie de l'information et de la communication (FEDICT) souhaite accéder aux registres Banque Carrefour visés à l'article 4 de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*.

Conformément à l'article 2, § 1^{er}, de l'arrêté royal du 11 mai 2001 *portant création du service public fédéral Technologie de l'information et de la communication*,

FEDICT a pour mission de développer une stratégie commune en matière d'e-government et d'en surveiller le respect, de promouvoir et de veiller à l'homogénéité et à la cohérence de la politique à l'aide de cette stratégie commune, d'assister les services publics fédéraux lors de la mise en œuvre de cette stratégie commune, de développer les normes, les standards et l'architecture de base nécessaires pour une mise en œuvre efficace de la technologie de l'information et de la communication à l'appui de cette stratégie et d'en surveiller le respect, de développer des projets et des services qui englobent potentiellement l'ensemble des services publics fédéraux et qui soutiennent cette stratégie commune et de gérer la collaboration avec les autres autorités en matière d'e-government et de technologie de l'information et de la communication.

- 1.2. Dans le cadre de l'élaboration de projets en matière d'e-government, il y a lieu d'exécuter plusieurs phases¹: la phase de développement d'une application informatique, la phase de test et éventuellement d'amélioration, la phase de mise en production et enfin la phase de gestion et de maintenance. En vue de la détection de problèmes, les applications informatiques font l'objet d'un monitoring durant la phase de gestion. Ces phases sont essentielles pour l'élaboration de projets en matière d'e-government et font partie des tâches essentielles de FEDICT.

FEDICT souhaite accéder aux données à caractère personnel des registres Banque Carrefour qui sont utilisées dans les applications informatiques qui sont liées aux registres Banque Carrefour via l'«*Universal Messaging Engine*» (UME), le «*Federal Service Bus*» (FSB) et/ou les services web. FEDICT doit tester, améliorer, maintenir ces applications et les soumettre à un monitoring.

FEDICT pourrait, de manière générale, dans le cadre des tests des applications informatiques, utiliser des données à caractère personnel de test fictives dans l'environnement d'acceptation et, de temps à autre, dans l'environnement de production. Dans le cadre du monitoring et de la résolution des problèmes constatés, FEDICT pourrait cependant, à titre exceptionnel, utiliser des données à caractère personnel réelles qui sont enregistrées dans les registres Banque Carrefour. Il s'agit in extenso des données à caractère personnel qui sont disponibles pour les utilisateurs des applications informatiques précitées, dans la mesure où ils y ont été autorisés par la section sécurité sociale du Comité sectoriel de la sécurité sociale et de la santé.

¹ Une application informatique est développée dans l'«*environnement de développement*», un système qui travaille de manière tout à fait autonome et qui n'a pas d'interaction avec d'autres systèmes (les développeurs sont les seuls à utiliser l'environnement de développement). Dès que les développeurs ont réalisé leur tâche, l'application informatique est copiée dans l'«*environnement de test*» dans lequel il est vérifié si elle répond aux besoins (l'interaction avec d'autres systèmes est aussi testée à cette occasion). Ensuite, l'application est transférée vers l'«*environnement d'acceptation*». Il s'agit de l'environnement auquel le demandeur même a accès pour accepter l'application informatique (c'est-à-dire qu'il peut y vérifier si elle fonctionne comme il le souhaite) et dans lequel des données à caractère personnel fictives sont utilisées. Lorsque le demandeur approuve l'application informatique, elle est enfin copiée dans l'«*environnement de production*» où elle peut être utilisée par tous les utilisateurs.

Par ailleurs, l'accès de FEDICT aux registres Banque Carrefour serait uniquement possible dans le cadre du monitoring des programmes informatiques permettant de communiquer des données à caractère personnel à un tiers, pour autant que ce tiers ait lui-même pris l'initiative de la communication, ait à cet égard constaté un problème et l'ait signalé à FEDICT en vue de trouver une solution. Cela signifie que ce n'est pas FEDICT mais bien le tiers en question qui détermine les personnes concernant lesquelles des données à caractère personnel issues des registres Banque Carrefour sont mises à la disposition de FEDICT.

- 1.3.** FEDICT utiliserait les données à caractère personnel à des fins de test, d'amélioration, de maintenance et de monitoring des applications informatiques qui ont une connexion avec les registres Banque Carrefour via l'UME, la FSB et/ou les services web.

L'UME est l'instrument qui a été développé par FEDICT permettant d'établir une connexion avec les différents systèmes des autorités fédérales et entre ceux-ci grâce aux messages électroniques standardisés. L'UME a entre temps évolué et est devenu le FSB, un portail qui regroupe plusieurs services web. Ces services web consistent en des applications informatiques qui servent souvent à rendre publiques les banques de données à caractère personnel authentiques. Ils permettent de demander à distance, à partir d'un ordinateur client, des données à caractère personnel auprès d'un serveur.

Certaines applications informatiques ont accès, via l'UME, le FSB et les services web, aux banques de données à caractère personnel authentiques, telles les registres Banque Carrefour. Les utilisateurs de ces applications informatiques y sont autorisés par le Comité sectoriel de la sécurité sociale et de la santé.

- 1.4.** En vue d'une prestation de services de qualité, FEDICT doit pouvoir tester régulièrement les applications informatiques, éventuellement les améliorer, les maintenir et les soumettre à un monitoring.

Lors des tests des applications informatiques, il est important de créer une situation qui ressemble le plus possible à une véritable transaction. Dans la mesure du possible, il serait fait usage de données à caractère personnel de test dans l'environnement d'acceptation (pendant la phase du développement d'une application informatique, il serait toujours fait appel à l'environnement d'acceptation). Cependant, lorsque ceci s'avère vraiment nécessaire pour une exécution efficace des tests d'une application informatique, des données à caractère personnel de test fictives pourraient être utilisées dans un environnement de production (à ce moment, il serait convenu avec la Banque Carrefour de la sécurité sociale, en ce qui concerne les registres Banque Carrefour, quelles données à caractère personnel de test fictives pourraient être utilisées dans l'environnement de production); ceci est le cas lorsqu'une nouvelle version d'une application informatique entre en production (il y a toujours lieu d'effectuer une fois un test afin de vérifier que tous les aspects sont effectivement en ordre) ou lorsque des

problèmes se présentent dans l’environnement de production qui ne peuvent être reproduits dans l’environnement de test (il y a lieu d’exécuter un “debugging” dans l’environnement de production). Parfois (mais à titre exceptionnel) des données à caractère personnel réelles seraient aussi utilisées dans l’environnement de production. Le monitoring permettrait d’accéder à des données à caractère personnel réelles figurant dans les registres Banque Carrefour au moment de la survenance d’un problème avec une application informatique (pour rappel, un tiers qui a des problèmes au moment d’accéder aux registres Banque Carrefour peut signaler cela à FEDICT, qui consulterait ensuite les registres Banque Carrefour en vue de la résolution de ces problèmes).

- 1.5.** FEDICT conserverait les données à caractère personnel issues des registres Banque Carrefour, en vue des tests, de l’amélioration, de la maintenance et du monitoring des applications informatiques, temporairement dans un environnement sécurisé. Les résultats des tests et du monitoring seraient analysés en vue de l’amélioration éventuelle des applications informatiques et en vue de la résolution des problèmes lors de leur fonctionnement.

FEDICT semble ne pas être en mesure de tester, d’améliorer et de maintenir les applications informatiques, s’il n’effectue pas sporadiquement un accès réel aux banques de données à caractère personnel authentiques (en l’occurrence, les registres Banque Carrefour). Les tests, l’amélioration, la maintenance et le monitoring des applications informatiques sont nécessaires en vue de garantir une prestation de services de qualité. Le fonctionnement efficace, la sécurité et la disponibilité permanente des applications informatiques s’en trouvent garantis.

Les tests, l’amélioration et la maintenance des applications informatiques ont généralement lieu à l’aide de données à caractère personnel fictives dans l’environnement d’acceptation ou dans l’environnement de production de la banque de données à caractère personnel authentique.

Dans le cadre de la résolution d’un problème qui a été détecté au cours du monitoring, un accès effectif aux données à caractère personnel réelles dans l’environnement de production s’avère parfois nécessaire. Cependant, les données à caractère personnel qui seraient demandées à l’occasion de problèmes constatés lors du monitoring d’une application informatique, seraient uniquement mises à la disposition des personnes y habilitées, c’est-à-dire des collaborateurs de FEDICT ou de son prestataire de services qui sont tenus d’en respecter la confidentialité.

- 1.6.** FEDICT sollicite une autorisation à durée indéterminée, étant donné que les tests, l’amélioration, la maintenance et le monitoring constituent une tâche essentielle de sa mission en matière d’e-government.

Les données à caractère personnel seraient conservées aussi longtemps que nécessaire pour les tests, l’amélioration et la maintenance des applications informatiques et pour la résolution de messages erreurs, et ce pendant un an au

maximum. En toute hypothèse, les données à caractère personnel seraient détruites suite à la réussite des tests ou suite à la résolution des erreurs constatées. Les loggings des activités de test seraient conservés de la même façon que les loggings des activités de production ordinaires.

2. EXAMEN DE LA DEMANDE

- 2.1.** Il s'agit d'une communication de données à caractère personnel qui, conformément à l'article 15, § 1^{er}, alinéa 2, de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, doit faire l'objet d'une autorisation de principe de la section sécurité sociale du Comité sectoriel de la sécurité sociale et de la santé.
- 2.2.** FEDICT offre des applications informatiques permettant d'accéder aux registres Banque Carrefour.

Cependant, les personnes physiques qui doivent être identifiées de façon univoque ne sont pas toutes enregistrées dans le Registre national des personnes physiques et ne possèdent pas toutes un numéro de registre national (par exemple, les travailleurs frontaliers qui séjournent à l'étranger mais qui travaillent en Belgique ou les personnes physiques qui ont droit à des prestations de la sécurité sociale belge mais qui n'ont jamais séjourné en Belgique). C'est la raison pour laquelle la Banque Carrefour de la sécurité sociale gère une banque de données à caractère personnel complémentaire. Les registres Banque Carrefour contiennent au maximum les données à caractère personnel suivantes relatives à ces personnes physiques: le nom, les prénoms, le lieu de naissance, la date de naissance, le sexe, la nationalité, la résidence principale, la date de décès et l'état civil et les modifications successives de ces données à caractère personnel.

Les personnes physiques qui, dans le passé, ont été inscrites dans le Registre national des personnes physiques et qui ont eu un numéro national mais dont les données d'identification ne sont, dans l'intervalle, plus actualisées par le Registre national des personnes physiques, sont aussi enregistrées dans les registres Banque Carrefour (avec maintien de leur numéro national). Dans la mesure où une personne physique qui est enregistrée dans les registres Banque Carrefour ne possède pas de numéro national, la Banque Carrefour de la sécurité sociale lui attribue un numéro Banque Carrefour.

L'accès aux registres Banque Carrefour requiert une autorisation préalable de la section sécurité sociale du Comité sectoriel de la sécurité sociale et de la santé. Tout utilisateur qui souhaite accéder aux registres Banque Carrefour au moyen d'une application informatique de FEDICT doit par conséquent disposer au préalable d'une telle autorisation.

- 2.3.** A l'heure actuelle, FEDICT souhaite lui aussi accéder aux données à caractère personnel contenues dans les registres Banque Carrefour, en vue du test, de l'amélioration, de la maintenance et du monitoring des applications informatiques. A cet effet, il est généralement fait usage de données à caractère personnel de test fictives mais l'usage de données à caractère personnel peut s'avérer nécessaire à titre exceptionnel. Ceci est le cas lors du monitoring d'applications informatiques à la demande d'un tiers qui utilise ces applications et qui est confronté à des difficultés concrètes (afin de faire face aux difficultés, FEDICT doit être en mesure de consulter les données à caractère personnel qui donnent lieu à ces difficultés).

La communication poursuit par conséquent une finalité légitime, à savoir l'exécution de tests, l'amélioration, la maintenance et le monitoring efficaces d'applications informatiques permettant aux utilisateurs y autorisés par le Comité sectoriel de la sécurité sociale et de la santé d'accéder aux registres Banque Carrefour.

Les données à caractère personnel communiquées sont pertinentes et non excessives par rapport à cette finalité. FEDICT n'utiliserait des données à caractère personnel réelles issues des registres Banque Carrefour qu'à titre exceptionnel, lorsque cela s'avère nécessaire pour la résolution de problèmes qui sont détectés lors du monitoring des applications informatiques.

Les données à caractère personnel en question seraient uniquement mises à la disposition des collaborateurs y habilités de FEDICT (ou de son prestataire de services) qui sont tenus d'en respecter la confidentialité et ne seraient conservées qu'aussi longtemps que nécessaire pour les tests, l'amélioration et la maintenance des applications informatiques et pour la résolution de messages erreurs, et ce pendant un an au maximum.

L'accès aux registres Banque Carrefour par FEDICT s'inscrit dans le cadre du monitoring des programmes informatiques par lesquels des données à caractère personnel sont communiquées à un tiers, pour autant que ce tiers ait lui-même pris l'initiative du monitoring, suite à la constatation d'un problème lors de la communication de données à caractère personnel. FEDICT doit pouvoir disposer des données à caractère personnel en question afin de résoudre le problème constaté.

- 2.4.** FEDICT fait déjà au maximum usage de données à caractère personnel de test dans l'environnement de test du registre national dans le cadre du test, de l'amélioration, de la maintenance et du monitoring des applications informatiques qui ont une connexion avec le registre national via l'UME, le FSB et/ou les services web. Il n'utilise l'environnement de production que dans des cas exceptionnels.

Par la délibération n° 19/2008 du 7 mai 2008, FEDICT a été autorisé par le comité sectoriel du Registre national à accéder aux données à caractère personnel réelles du registre national en vue de la réalisation de la finalité précitée.

Le comité sectoriel du Registre national a constaté que FEDICT devait certes pouvoir disposer, lors du test, de l'amélioration et du monitoring des applications informatiques, du même accès au registre national que celui dont disposent les instances auxquelles il offre des services mais que cet accès ne peut être illimité.

3. SÉCURITÉ DE L'INFORMATION

- 3.1.** Le Comité sectoriel de la sécurité sociale et de la santé prend acte du fait qu'un conseiller en sécurité de l'information a été désigné auprès de FEDICT.

Le conseiller en sécurité de l'information en question est chargé, en vue de la protection des données à caractère personnel qui sont traitées par son mandataire et en vue de la protection de la vie privée des personnes auxquelles ces données à caractère personnel ont trait, de fournir des avis qualifiés à la personne chargée de la gestion journalière et d'exécuter les missions qui lui ont été confiées par cette dernière. Il a une mission de conseil, de stimulation, de documentation et de contrôle en matière de sécurité de l'information.

Il remplit également la fonction de préposé à la protection des données, visé à l'article 17bis 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*.

Il est en outre chargé de l'exécution de la politique en matière de sécurité de l'information de son mandataire. Le cas échéant, il peut être fait appel à cet effet au document « Mesures de référence applicables à tout traitement de données à caractère personnel » de la Commission de la protection de la vie privée.

- 3.2.** FEDICT doit par ailleurs tenir compte des normes minimales de sécurité qui ont été définies par le Comité général de coordination de la Banque Carrefour de la sécurité sociale et qui ont été approuvées par le Comité sectoriel de la sécurité sociale et de la santé.
- 3.3.** FEDICT doit, au préalable, intégrer les intéressés dans le répertoire des références de la Banque Carrefour de la sécurité sociale, visé à l'article 6 de la loi du 15 janvier 1990.
- 3.4.** Auprès de la Banque Carrefour de la sécurité sociale sont tenus à jour des loggings des communications à FEDICT, dans lesquels sont notamment enregistrés quelles données à caractère personnel sont communiquées dans le cadre de la finalité précitée, concernant quelle personne et à quel moment. La Banque Carrefour de la sécurité sociale n'est toutefois pas en mesure de savoir à quel collaborateur concret de FEDICT (ou de son prestataire de services) les données à caractère personnel sont communiquées. FEDICT est tenu de conserver cela dans des loggings plus détaillés, contenant par communication une indication de quelle personne a obtenu

quelles données à caractère personnel concernant quelle personne à quel moment et pour quelle finalité.

Ces loggings doivent être conservés pendant dix ans au moins en vue du traitement de plaintes éventuelles ou de la constatation d'irrégularités éventuelles en ce qui concerne le traitement des données à caractère personnel.

Les loggings mêmes doivent être protégés au moyen de mesures garantissant la confidentialité, l'intégralité et la disponibilité. Ils sont transmis au Comité sectoriel de la sécurité sociale et de la santé et à la Banque Carrefour de la sécurité sociale à leur demande.

- 3.5.** Le comité sectoriel prend, en outre, connaissance du fait qu'une politique de sécurité de l'information, basée sur les principes des cercles de confiance, a été développée auprès de FEDICT. Les parties concernées par un échange de messages électroniques fixent des accords, ce qui permet de détecter, pour tout échange, les tentatives d'usage illégitime, de rendre les utilisateurs responsables pour leurs actes, de reconstruire les incidents possibles et de prouver que certaines conditions relatives au mode de conservation et de consultation de données à caractère personnel sont respectées.
- 3.6.** Les données à caractère personnel en question seront uniquement mises à la disposition des collaborateurs y habilités de FEDICT (ou de son prestataires de services) qui sont tenus d'en respecter la confidentialité.

Une liste des noms de ces collaborateurs qui, dans le cadre de l'exercice de leur fonction, ont accès aux données à caractère personnel qui sont enregistrées dans les registres Banque Carrefour est mise à la disposition par FEDICT.

Par ces motifs,

la section sécurité sociale du Comité sectoriel de la sécurité sociale et de la santé

autorise la Banque Carrefour de la sécurité sociale à accorder, aux conditions précitées, l'accès, dans le chef du service public fédéral Technologie de l'information et de la communication (FEDICT), aux registres Banque Carrefour, en vue du test, de l'amélioration, de la maintenance et du monitoring des applications informatiques permettant aux utilisateurs y habilités par le comité sectoriel d'accéder aux registres Banque Carrefour.

Yves ROGER
Président

<p>Le siège du Comité sectoriel de la Sécurité sociale et de la Santé est établi dans les bureaux de la Banque-Carrefour de la Sécurité sociale, à l'adresse suivante : Chaussée Saint-Pierre, 375 – 1040 Bruxelles (tél. 32-2-741 83 11)</p>
