



Recommandation n° 01/2012 du 18 janvier 2012

Objet: recommandation concernant la possibilité d'un inventaire des banques de données pertinentes et d'une amélioration de l'échange d'informations dans le cadre de la lutte contre la fraude sociale (CO-AR-2011-013)

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 30 ;

Vu la demande de Monsieur André Flahaut, Président de la Chambres des Représentants reçue le 24/10/2011;

Vu le rapport de Monsieur Stefan Verschuere;

Émet, le 18 janvier 2012, la recommandation suivante:

I. Contexte et objet de la demande

1. La Commission a été saisie par le Président de la Chambre des représentants, Monsieur André Flahaut, des questions de savoir dans quelle mesure il est possible :
 - que des instances publiques puissent disposer d'un inventaire des banques de données pertinentes afin de lutter contre la fraude sociale ;
 - d'améliorer l'échange des données à caractère personnel entre ces instances chargées de lutter contre la fraude sociale.
2. Ces questions font suite à une audition ayant eu lieu à la Chambre des représentants, le 11 octobre 2011, relative aux mercuriales du procureur général près de la cour d'appel d'Anvers et de l'avocat général près de la cour du travail d'Anvers, plus particulièrement en ce qui concerne la politique migratoire et ses conséquences sur le régime social (ci-après l'audition)¹.
3. Faute de précision quant à l'objet de la demande, la Commission se limitera à répondre aux remarques et questions relatives au sujet formulé par les divers intervenants lors du débat constituant l'objet de l'audition. Toutefois, la Commission estime utile de faire précéder les présentes recommandations très générales d'un rappel des dispositions et dispositifs existants pour ce qui concerne la lutte contre la fraude sociale à partir de l'exploitation des banques de données disponibles.

II. Réponse de la Commission quant à certaines remarques formulées lors de l'audition du 11 octobre 2011

4. A la page 20 de l'audition, la Commission est perçue comme constitutive d'un frein à l'élaboration de mesures efficaces afin de lutter contre la fraude sociale. Il est ainsi fait mention du refus prononcé par le Comité sectoriel pour l'Autorité Fédérale, en date du 9 juin 2011, de voir la banque de données de l'Agence Fédérale pour l'accueil des demandeurs d'asile (ci-après "Fedasil") être consultée par l'Office des Etrangers.
5. Prétendre que la Commission a interdit un échange d'informations ne repose sur aucun fondement de fait. Le Comité sectoriel pour l'Autorité Fédérale a clairement affirmé à ce sujet que l'Office des étrangers pouvait réclamer les données de localisation en vertu de sa

¹ Audition relative aux mercuriales du procureur général près de la cour d'appel d'Anvers et de l'avocat général près de la cour du travail d'Anvers, plus particulièrement en ce qui concerne la politique migratoire et ses conséquences sur le régime social, Chambre des représentants de Belgique, 11 octobre 2011, Doc 53 (1787/001).

compétence de police administrative spéciale². Le fait que l'Office des étrangers n'ait reçu aucune autorisation du Comité sectoriel reposait sur la constatation que l'Office des étrangers devait, de droit, aller chercher ces données dans le "registre d'attente" en tant que source authentique et que ladite banque de données de Fedasil n'était pas techniquement et institutionnellement en mesure de bien organiser une telle consultation³.

6. A la page 40 de l'audition, un intervenant suggère la création d'une banque de données qui reprendrait *"les données concernant toutes les personnes soutenues par les CPAS, de sorte que le travail d'enquête ne doive pas être recommencé en cas de déménagement et que les possibilités de falsification soient réduites"*.
7. A cet égard, la Commission recommande de ne pas créer une telle banque de données centralisée qui stockerait une multitude d'informations dans la mesure où il existe des fichiers disposant déjà de telles informations. Elle préconise plutôt de poursuivre le développement des systèmes existants qui ont fait leur preuve et de les connecter entre eux via une application spécifique qui permettrait de lutter contre la fraude sociale, si cela s'avère nécessaire au cas où aucun système ne le permettrait encore actuellement (voir ci-dessous les points 25 et suivants).

III. La Banque Carrefour de la Sécurité Sociale et le Comité sectoriel de la sécurité sociale et de la santé

A. La Banque Carrefour de la Sécurité Sociale

8. La Banque Carrefour de la Sécurité sociale (ci-après BCSS) est un organisme public, institué par la loi organique du 15 janvier 1990 de la Banque Carrefour de la sécurité sociale, qui a développé un réseau électronique reliant les différentes institutions de sécurité sociale.
9. Au sein du réseau, la Banque Carrefour fait office de moteur dans une dynamique de partage de l'information relative aux assurés sociaux et aux employeurs. Chaque institution de sécurité sociale est responsable de l'enregistrement et de la tenue à jour des

² Voir en la matière la délibération AF n° 12/2011 du 9 juin 2011, publiée sur le site Internet de la CPVP, en particulier le point 12 : "12. Les agents de l'Office des étrangers disposent à cet effet de pouvoir d'investigation. En effet, l'article 81 de la loi du 15 décembre 1980 prévoit que les infractions à son encontre sont recherchées et constatées par, entre autres, les agents de l'Office des étrangers. Ces derniers rassemblent les preuves des infractions et en livrent les auteurs aux autorités judiciaires, conformément aux dispositions du Code d'instruction criminelle."

D'ailleurs, ce droit à l'information a encore été confirmé dans la lettre du 17 juin 2011 du Président de la Commission au Directeur général de l'Office des étrangers.

³ L'avis de FEDICT a été suivi à cet égard. Celui-ci affirmait en effet qu' "aucune véritable banque de données au sens strict du terme n'était disponible au sein de Fedasil mais uniquement des spreadsheets."

informations contenues dans sa banque de données. Sur base d'autorisations très strictes, les informations contenues dans les différentes banques de données sont accessibles aux autres institutions de sécurité sociale via le réseau ; ceci évite les collectes multiples de données identiques. Les données sociales à caractère personnel sont conservées et gérées par l'institution qui, selon la nature des données, est la plus à même de les exploiter.

10. En vue d'un échange automatisé de données à caractère personnel, la Banque Carrefour dispose d'une banque de données qui ne contient pas d'informations de fond, mais uniquement des données de référence, qui indiquent par personne quelles données sont tenues dans quels régimes ou institutions de sécurité sociale et peuvent être obtenues.
11. Lorsqu'une institution de sécurité sociale a besoin de certaines données pour l'exécution de sa mission, elle est obligée d'adresser sa demande par voie électronique à la Banque Carrefour. Grâce au répertoire de référence et de localisation dont elle dispose, la Banque Carrefour peut vérifier si les données recherchées sont déjà disponibles dans une autre institution de sécurité sociale intégrée dans le réseau d'informations distribuées. Dans l'affirmative, elle se charge de mettre à la disposition de l'institution demanderesse les données nécessaires qui sont disponibles dans une autre institution de sécurité sociale. Ce n'est que lorsque les données sollicitées ne sont pas encore disponibles dans le réseau que l'institution demanderesse peut les demander directement à l'employeur ou à l'assuré social. De ce fait, différentes institutions ne demandent pas plusieurs fois à la même personne les mêmes données⁴.
12. Lors de l'élaboration de la loi organique de la Banque Carrefour, le législateur a consacré une attention particulière à la protection de la BCSS, de son réseau ainsi que des données personnelles qui sont échangées via ce réseau. La BCSS dispose d'un mécanisme de surveillance et l'échange de toutes données à caractère personnel est soumis à un mécanisme d'autorisation (voir ci-dessous le Comité sectoriel de la sécurité sociale et de la santé). Toutefois, ces mesures n'empêchent nullement de mener une lutte efficace contre la fraude sociale.
13. D'ailleurs le contrat d'administration entre l'Etat fédéral et la BCSS prévoit explicitement (en son article 44) que *"la BCSS établira, chaque année, à l'attention des Ministres concernés, un rapport sur les initiatives prises (et à prendre) et les résultats engrangés concernant la lutte contre la fraude sociale, les indus et les erreurs et l'analyse et la constatation des phénomènes de fraude, d'indus et d'erreur"*.

⁴ Informations issues du site web de la BCSS

http://www.ksz.fgov.be/fr/bcss/page/content/websites/belgium/about/inshort/inshort_01.html

B. Le Comité sectoriel de la sécurité sociale et de la santé

14. La communication de données sociales à caractère personnel par des institutions de sécurité sociale à d'autres instances situées dans ou à l'extérieur du réseau, doit faire l'objet d'une autorisation du Comité sectoriel de la sécurité sociale et de la santé (ci-après CSSS). Sauf quelques exceptions prévues dans la législation, le Comité sectoriel autorise préalablement l'échange de tous les types de flux de données sociales entre institutions de sécurité sociale ainsi que l'échange de flux provenant des institutions à destination de personnes n'appartenant pas au réseau de la Banque Carrefour.
15. Le CSSS accorde ainsi régulièrement de nombreuses autorisations qui poursuivent la finalité de lutter contre la fraude sociale (voir ci-dessous point IV). Le CSSS n'a d'ailleurs, jusqu'à présent, jamais refusé aucun échange de données soumis à son autorisation afin de lutter contre la fraude sociale. La Commission elle-même récemment rendu un avis positif concernant des amendements au projet de loi portant des dispositions fiscales et diverses qui ont, entre autres, pour finalité de lutter contre la fraude sociale⁵.

IV. Dispositifs existants afin de lutter contre la fraude sociale

16. La BCSS a déjà mis en place des systèmes de détection de la fraude tant par des échanges de données entre les acteurs de la sécurité sociale que par des échanges de données avec des sources authentiques en dehors de son réseau (en particulier avec le SPF Finances).
17. Le rapport annuel relatif à la lutte contre la fraude sociale, les indus et les erreurs pour la période 2010-2012 rédigé par la BCSS en vertu de l'article 44 du contrat d'administration qui lie l'Etat fédéral et la BCSS (en annexe de la présente recommandation) liste ces divers dispositifs. A titre d'exemple, les dispositifs suivants ont déjà été autorisés par le CSSS et mis en place par la BCSS :
 - la banque de données "Oasis"⁶, qui contient des données à caractère personnel relatives à des employeurs identifiés des banques de données à caractère personnel existantes. Cette banque de donnée permet aux services concernés (l'inspection sociale auprès du Ministère des Affaires Sociales, de la Santé Publique et de l'Environnement, du Ministère de l'Emploi et du Travail, de l'ONSS et de l'ONEM) de réaliser des contrôles ciblés sur la base d'indicateurs potentiels

⁵ Avis n° 33/2011 du 30 novembre 2011 concernant les projets d'amendement au projet de loi portant des dispositions fiscales et diverses : enregistrement électronique des présences sur les chantiers temporaires ou mobiles et responsabilité solidaire relative au paiement du salaire minimum.

⁶ Organisation Anti-fraude des Services d'Inspection Sociale.

de fraude à partir d'un datawarehouse contenant des données classées, regroupées et codées provenant des banques de données sociales existantes⁷. Ce transfert de données a été autorisé par le Comité de surveillance⁸ et élargit, entre autres, aux données sociales à caractère personnel relatives au chômage temporaire par le Comité sectoriel de la sécurité sociale⁹;

- le projet Genesis qui vise à optimiser la lutte contre la fraude sociale et à harmoniser les moyens de fonctionnement des services d'inspection concernées¹⁰;
- la consultation de diverses banques de données sociale par les services d'inspection de la Direction générale Contrôle des lois sociales (du SPF Emploi, travail et concertation sociale), de l'inspection sociale (SPF Sécurité sociale), de l'ONSS, de l'ONSSAPL, de l'ONEM et du Fonds des accidents du travail (FAT)¹¹.

18. Des initiatives sont également en cours actuellement auprès de la BCSS (voir le rapport en annexe pour d'avantage de précision).

V. Recommandation générale concernant la lutte contre la fraude sociale au regard de la loi vie privée

A. Application de la Loi vie privée

19. L'article 8 de la Convention européenne des droits de l'Homme ainsi que l'article 22 de la Constitution garantissent le droit à la protection de la vie privée et familiale. Ils stipulent que toute ingérence dans ce droit à la vie privée ne peut avoir lieu que sur base d'une loi, d'un décret ou d'une ordonnance.
20. La création de banques de données rassemblant des données personnelles ainsi que l'échange de données personnelles aux fins de lutter contre la fraude sociale constituent des traitements de données à caractère personnel rentrant dans le champ d'application de la loi vie privée, ce qui implique le respect par le responsable du traitement de l'ensemble des principes qu'elle édicte.

⁷ Il s'agit notamment des banques suivantes : le répertoire des employeurs (ONSS), le LATG (ONSS), la banque de données DIMONA (ONSS), le fichier "chantiers et sous-traitants", le fichier "entrepreneurs en règle" (ONSS), le fichier "comptes" (ONSS), le fichier "recouvrement" (ONSS), le fichier des procès-verbaux des inspecteurs sociaux du Ministère des Affaires sociales, de la Santé publique et de l'Environnement et le fichier "chômeurs" (ONEM).

⁸ Délibération 01/06 du 6 mars 2001 du Comité de surveillance.

⁹ Délibération n° 05/001 du 18 janvier 2005 du Comité sectoriel de la sécurité sociale.

¹⁰ Délibération N° 04/044 DU 7 décembre 2004 du Comité sectoriel de la sécurité sociale.

¹¹ Délibération n° 04/032 du 5 octobre 2004 du Comité sectoriel de la sécurité sociale.

B. Finalité – Licéité – Proportionnalité

1. Finalité et licéité

21. L'article 5 de la loi vie privée énonce les hypothèses dans lesquelles un traitement de données à caractère personnel peut être réalisé. La création de banques de données à caractère personnel et l'échange de telles données aux fins de lutter contre la fraude sociale pourrait rentrer dans les hypothèses prévues aux articles 5, c) et e) car ces traitements seraient nécessaires au respect d'une obligation à laquelle le responsable du traitement est soumis par ou en vertu d'une loi, d'un décret ou d'une ordonnance ou/et nécessaires à l'exécution d'une mission d'intérêt public dont est investi le responsable du traitement¹².
22. De plus, et conformément à l'article 4, § 1, 2°, de la LVP, les données à caractère personnel doivent être obtenues pour des finalités déterminées et explicites et ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités. Les données seront ici traitées aux fins de lutter contre la fraude sociale. Il convient toutefois de décrire, lors de la mise en place du traitement cette finalité de la manière la plus précise, détaillée et complète que possible et ce, afin de répondre au droit des citoyens d'être informés des traitements qui peuvent être effectués sur leurs données à caractère personnel. Une telle description des finalités ne doit toutefois pas être réalisée par une loi. Elle peut intervenir, par exemple, par le biais d'un acte réglementaire ou encore par une autorisation d'un des comités sectoriels institués auprès de la Commission.

2. Proportionnalité

23. L'article 4, § 1, 3°, de la LVP stipule que les données à caractère personnel doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement. Dans le choix des modalités de traitement permettant d'atteindre la finalité poursuivie, le responsable du traitement devrait également veiller à opter pour celles qui sont les moins attentatoires à la vie privée des personnes concernées. Une ingérence dans le droit à la protection des données des personnes concernées doit en effet être proportionnée au regard des finalités du traitement pour le responsable du traitement.

¹² Si les données ainsi traitées sont des données sensibles au sens de l'article 6 de la LVP ou des données relatives à la santé, leur traitement ne peut être admis que s'il est effectué dans une des hypothèses limitativement prévues aux articles 6 § 2 et 7 § de la LVP.

24. Lors de l'éventuelle création d'une banque de données ou lors de l'échange de données à caractère personnel, le responsable du traitement devra donc s'assurer de ne requérir que des données adéquates, pertinentes et non excessives au regard de la finalité ainsi poursuivie.

3. Création d'une nouvelle banque de données

25. Quant à la création d'une nouvelle banque de données à caractère personnel aux fins de lutter contre la fraude sociale, la Commission insiste sur le principe, souvent souligné dans la jurisprudence de la Commission de la protection de la vie privée, selon lequel les données doivent en principe toujours être réclamées auprès de la source authentique.
26. La Commission est d'avis qu'il faut éviter la concentration d'information dans une banque de données supplémentaire sauf si certaines informations ne sont actuellement détenues dans aucune banque de données.
27. Par ailleurs, on a établi de longue date un système modèle¹³ qui évite la concentration des données et qui permet sans doute plus efficacement, que si un fichier central était constitué, de connecter entre-elles toutes les bases de données existantes dès lors que cette interconnexion poursuit une finalité légitime ; ce qu'est la lutte contre la fraude sociale.
28. La Commission estime en effet qu'il est plus efficace de procéder par interconnexion de banques de données existantes car la consultation d'un fichier central à partir d'autres banque de données actives ne permet pas de garantir la plus grande exactitude des informations traitées. L'exactitude du fichier dépend de la qualité des mises à jour effectuées. Le fichier initial est, en toute hypothèse, censé fournir l'information disponible la plus exacte.
29. De surcroit, un système d'interconnexion de banques de données existantes offre une meilleure sécurité que la création d'une grande banque de données. En effet, le système d'interconnexion permet au responsable du traitement de contrôler les flux et l'identité des personnes ayant eu accès aux données. Un tel système permet également de limiter la perte des données ou la diffusion de ces dernières dans le cas éventuel ou une défaillance du système de sécurité devait survenir.

¹³ A savoir le réseau de la BCSS.

C. Transparence

30. En vertu de l'article 9 de la LVP, diverses informations doivent être communiquées à la personne concernée au sujet du traitement envisagé (responsable du traitement, finalités, destinataires des données, ...) lors de l'obtention des données la concernant.
31. Le paragraphe 2 de cet article 9 prévoit deux exceptions à cette obligation d'information lorsque les données ainsi obtenues n'ont pas été collectées auprès de la personne concernée. Ainsi, le responsable du traitement est dispensé de fournir les informations précitées lorsque le traitement est effectué en vue de l'application d'une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance.
32. Au vu de ce qui précède, et dans le cas où l'exception ainsi prévue par la loi vie privée ne trouve pas à s'appliquer, la Commission insiste sur l'importance qu'une information claire et détaillée soit communiquée aux personnes dont les données seront traitées dans le cadre de la lutte contre la fraude sociale.

D. Délai de conservation

33. Conformément à l'article 4, § 1, 5°, de la LVP, les données ne peuvent pas être conservées sous une forme permettant l'identification des personnes concernées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement.
34. Il appartient dès lors au responsable du traitement ultérieur de prévoir un délai de conservation adéquat au regard de cet article 4, § 1, 5°.

E. Sécurité des données

35. En vertu de l'article 16 de la LVP, le responsable du traitement a l'obligation de prendre toutes les mesures techniques et organisationnelles nécessaires pour assurer la sécurité des données. La Commission se réfère à ce titre aux « mesures de référence en matière de sécurité applicables à tout traitement de données à caractère personnel » figurant sur son site web¹⁴. La Commission souhaite également recommander les normes minimales de sécurité qui ont été définies par le Comité général de coordination de la Banque Carrefour

¹⁴ <http://www.privacycommission.be/fr/static/pdf/mesures-de-reference-vs-01.pdf>

de la sécurité sociale et qui ont été approuvées par le comité sectoriel de la sécurité sociale et de la santé^{15 16}.

F. Autorisations des comités sectoriels

36. Comme indiqué au point 14, en vertu de l'article 15 de la loi organique du 15 janvier 1990 de la BCSS, la section sécurité sociale du comité sectoriel de la sécurité sociale et de la santé doit accorder une autorisation de principe (sauf pour quelques exceptions prévues dans la législation) pour toute communication de données à caractère personnel par la BCSS ou par des institutions de sécurité sociale à d'autres instances situées dans ou à l'extérieur du réseau. Le comité sectoriel de la sécurité sociale et de la santé a pour mission de s'assurer que les principes de finalité, proportionnalité, transparence ainsi que les mesures de sécurité sont bien respectés.
37. Si le traitement de données envisagé nécessite d'avoir accès aux informations enregistrées dans le Registre national et/ou d'utiliser le numéro de Registre national, le responsable du traitement devra également obtenir une autorisation du comité sectoriel du registre national (articles 5 et 8 de la loi du 8 août 1983 organisant un registre national des personnes physiques).
38. Il se peut également qu'un tel traitement soit soumis à l'autorisation du comité sectoriel pour l'autorité fédérale si la communication électronique de données personnelles envisagées dans le traitement est effectuée par un service public fédéral ou par un organisme public avec personnalité juridique qui relève de l'autorité fédérale (article 36 bis de la LVP). Ce comité dispose d'une compétence résiduaire, il n'intervient que si la communication de données n'a pas déjà fait l'objet d'une autorisation de principe d'un autre comité sectoriel.

VI. CONCLUSION

¹⁵ http://www.ksz-bcss.fgov.be/binaries/documentation/fr/secure/normes_minimales_securite.pdf

¹⁶ Dans le contexte de la révision du cadre réglementaire de la protection des données de l'Union européenne, il est envisagé de rendre obligatoires la désignation d'un Data Protection Officer (DPO – préposé à la protection des données selon la terminologie actuellement utilisée par la Loi belge) et la réalisation d'un Privacy Impact Assessment (PIA) dans des circonstances précises au nombre desquelles figure la réalisation de traitements de données visant à analyser et /ou prédire le comportement de personnes ; analyse ou prédiction pouvant résulter en des mesures produisant des effets juridiques à l'égard de celles-ci. Quelle que soit l'issue de ces propositions, la Commission de la protection de la vie privée recommande la mise en place de ces mesures destinées à renforcer la protection de la vie privée et des données personnelles des personnes dans le contexte de la lutte contre la fraude.

La Commission estime que les présents principes représentent les lignes directrices à respecter pour tous échanges de données à caractère personnel aux fins de lutter contre la fraude sociale et lors de l'éventuelle création de banques de données rassemblant des données à caractère personnel.

L'Administrateur ff,

Le Président,

(sé) Patrick Van Wouwe

(sé) Willem Debeuckelaere

Rapport annuel relatif à la lutte contre la fraude sociale, les indus et les erreurs en vertu de l'article 44 du contrat d'administration entre l'Etat fédéral et la Banque-carrefour de la sécurité sociale pour la période 2010-2012

1. Contrat d'administration

En vertu de l'article 44 du contrat d'administration entre l'Etat fédéral et la Banque Carrefour de la sécurité sociale pour la période 2010-2012, "la Banque-carrefour établira, chaque année, à l'attention des Ministres concernés, un rapport sur les initiatives prises (et à prendre) et les résultats engrangés concernant la lutte contre la fraude sociale, les indus et les erreurs et l'analyse et la constatation des phénomènes de fraude, d'indus et d'erreur".

2. Environnement existant et services

Dans le cadre de la lutte contre la fraude sociale, les erreurs et les indus, il est, dans un premier temps, essentiel de souligner les réalisations générales de la Banque Carrefour de la sécurité sociale (BCSS), à savoir:

- une clé d'identification unique
 - o pour chaque citoyen, lisible de façon électronique à partir de la carte d'identité sociale (carte SIS) et de la carte d'identité électronique ;
 - o pour chaque entreprise et chaque établissement d'une entreprise.
- une répartition des tâches entre les acteurs du secteur social et d'autres instances en ce qui concerne la gestion et l'enregistrement électronique de données sous forme authentique;
- environ 700 millions d'échanges électroniques de données à l'aide de plus de 220 messages structurés entre l'ensemble des acteurs du secteur social connectés au réseau;
- plus de 20 millions de transactions électroniques entre, d'une part, les acteurs du secteur social et, d'autre part, les entreprises et les citoyens
 - o soit par l'échange de messages électroniques structurés;
 - o soit via un portail intégré;
- un portail intégré avec
 - o des données relatives à tous les aspects de la sécurité sociale;
 - o des transactions électroniques pour entreprises, citoyens et professionnels du secteur social (e.a. fonctionnaires des villes/communes);
 - o des instructions harmonisées relatives aux transactions électroniques;
 - o une page personnelle pour chaque entreprise et chaque professionnel du secteur social en vue de la mise à la disposition électronique de documents ou de résultats de traitement provenant d'un acteur du secteur social, à l'occasion de l'utilisation d'une application par un utilisateur;
 - o exploitabilité de services de base lors de l'offre ou de l'utilisation de transactions électroniques;
- un eWorkspace intégré pour les professionnels du secteur social avec
 - o des e-teams;
 - o un workflow commun pour l'ensemble des acteurs sociaux (p.ex. e-leg);
- un centre de contact multimodal intégré Eranova qui est soutenu par un outil de gestion des relations-clients et qui travaille sur la base de service level agreements stricts.

Il est dès lors évident que, d'une part, l'extension systématique du réseau de la BCSS (nombre de messages et de destinataires) permettant la mise à disposition de données de sources authentiques, et, d'autre part, l'échange de données avec les entreprises et les citoyens via un portail intégré donnent *de facto* lieu à une amélioration à la fois sur le plan de la prévention et de la détection de fraude, d'erreurs et d'indus éventuels et, le cas échéant, de la réduction de ses dommages. A cet égard, il est, bien entendu, tenu compte de la loi du 15 janvier 1990 *relative à l'institution et à l'organisation d'une Banque-carrefour de la sécurité sociale*, 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*, de leurs arrêtés d'exécution et de toute autre disposition légale ou réglementaire relative à la protection de la vie privée.

3. Méthodes permettant d'éviter la fraude, les erreurs et les indus

Tout d'abord, il y a lieu d'éviter la fraude. Ceci est principalement possible grâce à la gestion coordonnée des informations telle que précitée. Songeons notamment à :

- l'identification unique de chaque citoyen et de chaque entreprise;
- l'impossibilité d'inscrire, dans le répertoire des références, une même personne, sous une même qualité, pour la même période, auprès de plusieurs institutions de la même branche de la sécurité sociale;
- les déclarations immédiates, voire préalables de faits aux acteurs du secteur social (p.ex. DIMONA/LIMOSA);
- l'utilisation des mêmes informations pour le calcul des cotisations et des indemnités;
- l'accès par les acteurs qui octroient des droits aux données relatives aux droits dans d'autres branches de la sécurité sociale (éviter un cumul illicite d'allocations);
- l'accès public aux données relatives aux dettes d'entreprises auprès de la sécurité sociale, couplées dans le secteur de la construction à une responsabilité solidaire pour des clients potentiels et une obligation de retenue pour les clients des entreprises qui ont des dettes auprès de la sécurité sociale,
- le contrôle de qualité formel par ceux qui sont chargés de recueillir les données avant leur transmission, ce qui permet d'éviter la fraude, les erreurs et les indus.

4. Méthodes de lutte contre la fraude, les erreurs et les indus

Outre les méthodes permettant d'éviter la fraude, les erreurs et les indus, un soutien est également offert à un système de détection efficace de la fraude, des erreurs et des indus. Ceci vaut tant pour les échanges de données entre les acteurs de la sécurité sociale que pour des échanges de données avec des sources authentiques en dehors du réseau, en particulier avec le SPF Finances. Les projets énumérés ci-après ont donc été mis en place via le réseau de la BCSS, tant dans le cadre d'une prestation de service effective et efficace, d'une part, que dans le cadre de la lutte contre la fraude, les erreurs et les indus, d'autre part :

- la consultation des banques de données TAXI_AS auprès du SPF Finances est désormais possible pour les institutions de sécurité sociale ; la banque de données comprend toutes les données de la déclaration fiscale; les institutions de sécurité sociale suivantes ont accès à la consultation de TAXI_AS:
 - o le SPF Sécurité sociale – la DG Personnes handicapées;
 - o le SPF Sécurité sociale pour l'allocation d'aide aux personnes âgées;
 - o l'Institut national d'assurance maladie-invalidité (INAMI) – le service de contrôle administratif;

- les CPAS via le SPP Intégration sociale pour ce qui concerne l'allocation de chauffage;
- la BCSS dans le cadre des réductions forfaitaires pour le gaz et l'électricité;
- l'Office national des pensions (ONP) pour les dossiers revenu garanti aux personnes âgées et garantie de revenus pour personnes âgées;

le nombre de consultations s'élevait à 490.097 en 2010;

- la consultation de la banque de données CADNET auprès du SPF Finances est désormais également possible pour les institutions de sécurité sociale ; cette banque de données comprend, par personne physique et par personne morale, les données relatives à leur patrimoine immobilier (e.a. identification, nature du bien, revenu cadastral, portée du droit); des services web spécifiques ont été développés à l'attention de l'Office national de sécurité sociale (ONSS) et de l'ONP en vue de la consultation de cette banque de données; le nombre de consultations s'élevait à 68.668 en 2010;
- la notification sociale, aussi appelée projet de la "quatrième voie", permet un meilleur recouvrement des cotisations sociales au profit de l'ONSS, de l'Institut national d'assurances sociales pour travailleurs indépendants (INASTI) et des caisses d'assurances sociales pour travailleurs indépendants ; lors de la vente publique de biens mobiliers ou lors de la passation d'actes d'aliénation ou d'affectation hypothécaire de biens immobiliers, il est développé entre les fonctionnaires publics ou les officiers ministériels concernés et les institutions de sécurité sociale précitées un échange de données afin de connaître les dettes sociales éventuelles et, le cas échéant, de procéder à une saisie-arrêt ; le nombre de messages s'élevait à 8.555 en 2010 ;
- le projet "ePV" prévoit l'instauration d'un modèle électronique uniforme de PV pour les services d'inspection. A cet effet, une application web a été développée sur le portail de la sécurité sociale; celle-ci est utilisée depuis fin 2010 par les services d'inspection de l'ONSS, de l'Office national de l'emploi (ONEm), du SPF Sécurité sociale et du SPF Emploi, Travail et Concertation sociale (SPF ETCS). Dans un premier temps, les données relatives à ces PV électroniques seront transmises via la BCSS à la Direction des amendes pénales et, dans une phase ultérieure, au SPF Justice à l'attention des auditeurs du travail. Le projet vise à une meilleure qualité des PV et à un traitement plus efficace des PV auprès des différents acteurs concernés.
- dans le cadre du recouvrement fiscal et non fiscal, il est développé au profit du SPF Finances un service intégré d'accès à plusieurs banques de données au sein du secteur social (répertoire des employeurs, DmfA, fichier du personnel auprès de l'Office national de sécurité sociale des administrations provinciales et locales (ONSSAPL) et pécules de vacances auprès de l'Office national des vacances annuelles (ONVA)) ; ce service a été mis en production à la BCSS fin 2010, cependant celui-ci se trouve encore dans une phase d'évaluation auprès du SPF Finances;
- afin de simplifier la saisie-arrêt entre les mains de l'ONVA au bénéfice du SPF Finances, il a été développé un flux de données entre l'ONVA et le SPF Finances. Ce flux de données prévoit une actualisation annuelle des dettes fiscales et/ou non fiscales dont la retenue est demandée sur le pécules de vacances; le nombre de messages s'élevait à 68.976 en 2010.

- créé dans le cadre d'un projet de lutte anti-fraude commun aux divers services d'inspection, le datawarehouse OASIS a pour objectif de permettre aux services d'inspection sociale précités d'effectuer des analyses sur des données codées provenant de divers acteurs du secteur social en vue de détecter des fraudes potentielles (25.892.405 messages). En ce qui concerne les personnes soupçonnées de fraude sur base d' « avertisseurs » prédéfinis, des contrôles individuels ciblés sont effectués ;
- le projet « GENESIS » vise à optimiser la lutte contre la fraude sociale et à harmoniser les moyens de fonctionnement des services d'inspection concernés. Les divers services d'inspection ont donc, dans un premier temps, créé un « cadastre des enquêtes » qui leur permet de collaborer d'une manière plus efficace, de sorte que les informations recueillies puissent être mises à la disposition des services d'inspection concernés d'une manière uniforme. Ainsi, les services d'inspection peuvent vérifier si des enquêtes ont déjà été réalisées concernant un employeur donné. De la sorte, on évite qu'un même travail soit réalisé deux fois ;
- en vue d'optimiser la détection d'éventuelles fraudes, une transmission unique de données sociales au niveau de l'employeur a été opérée, au profit du SPF Finances, en ce qui concerne les secteurs du nettoyage industriel et du transport routier ; il s'agit de données relatives aux « avertisseurs » précités de OASIS, au chômage économique, au contrôle croisé DmfA-DIMONA, au répertoire des employeurs et à la DmfA. Cette communication portait sur environ huit cents employeurs du secteur des transports routiers et sur une trentaine d'employeurs du secteur du nettoyage industriel ;
- la BCSS apporte sa collaboration à la réalisation d'un projet d'échange de données entre l'ONEm et le SPF Finances concernant les entreprises de titres-services. Ce projet a deux objectifs : d'une part, permettre à l'ONEm de gérer plus efficacement les conditions d'agrément des entreprises de titres-services, notamment en ce qui concerne l'aspect des dettes fiscales et, d'autre part, permettre au SPF Finances d'optimiser la détection d'éventuelles fraudes fiscales ;
- en vue d'optimiser la détection d'éventuelles fraudes fiscales dans le cadre du traité de double imposition Belgique-France, une concertation a eu lieu entre l'ONSS et le SPF Finances concernant un échange de données relatives aux travailleurs frontaliers. Il est à noter qu'il ne s'agit pas de données individuelles relatives aux travailleurs, mais de données au niveau de l'employeur. Un accord est intervenu en ce qui concerne le contenu du flux de données ;
- dans le cadre d'une détection d'éventuelles fraudes concernant le « portage salarial » (un régime qui permet aux indépendants de se présenter en qualité de salariés), une sélection est préparée dans le cadastre LIMOSA au profit du SPF Finances. Cette sélection concerne un certain nombre de secteurs sensibles en matière de fraude. Le cadastre LIMOSA contient des informations relatives à l'occupation étrangère en Belgique. Tout travailleur salarié, indépendant ou stagiaire qui vient travailler temporairement en Belgique, doit dorénavant faire l'objet d'une déclaration électronique par le biais de l'application en question, sauf s'il en est exempté. Le projet LIMOSA a été élaboré sous la direction de l'ONSS et de la BCSS, en collaboration avec de nombreux autres acteurs du secteur social ;

- la BCSS apporte sa collaboration au projet "Datamining assuré social", lancé sous la direction de l'ONEM; l'objectif du projet est de générer, en croisant des données de différentes banques de données des institutions de sécurité sociale, du SPF Finances et du SPF Intégration sociale, Lutte contre la pauvreté, Economie sociale et Politique des grandes villes, des avertisseurs susceptibles de prouver des systèmes de fraude auprès de l'assuré social. Des profils de risque théoriques de l'assuré social ont entre-temps été inventoriés. 17 avertisseurs de fraude éventuelle ont été définis sur base de ces profils;
- la BCSS participe évidemment activement au Collège pour la lutte contre la fraude fiscale et sociale, au sein duquel sont abordés divers services évoqués dans le présent rapport ;
- un accord de coopération a été signé afin d'optimiser l'échange et l'utilisation de données fiscales et sociales. Plus concrètement, il s'agit surtout de l'échange réciproque d'informations disponibles relatives aux révisions fiscales et sociales de rémunérations et d'autres avantages imposables. Les parties signataires sont l'Administration de la fiscalité des entreprises et des revenus (AFER) du SPF Finances, le SPF ETCS, le SPF Sécurité sociale, l'ONSS, l'ONEm, l'INAMI et le Service de recherche et d'informations sociales (SIRS).

5. Initiatives en cours

Les services ci-après seront notamment finalisés au cours des prochaines années :

- accès à la banque de données TAXI-AS dans le chef de l'ONEm, de l'INASTI, de la DG Politique sociale, des CPAS et des services des institutions régionales;
- accès à la base de données CADNET dans le chef de l'INASTI et des CPAS;
- connexion du SPF Justice au réseau de la sécurité sociale, à la condition que le SPF Justice mette à disposition les moyens nécessaires;
- flux de données entre l'ONEm et le SPF Finances concernant les titres-services;
- transmission, de l'ONSS au SPF Finances, de données relatives aux travailleurs frontaliers au niveau de l'employeur.

La BCSS apporte également sa collaboration dans le cadre d'un accord de collaboration international relatif à la lutte contre la fraude. Ainsi, elle souhaite par exemple mettre en place en 2011 un échange de données entre l'ONP et son pendant allemand, la DRV (« Deutsche Rentenversicherung »), dans le cadre de la lutte contre la fraude au niveau des pensions payées à l'étranger. Le but est d'obtenir, les uns des autres, des données relatives au décès de leurs clients résidant dans l'autre pays (belges pensionnés résidant en Allemagne et vice versa).

6. Résultats atteints

La BCSS apporte sa collaboration en veillant à ce que tous les acteurs concernés puissent accéder aux données qui leur sont nécessaires dans le cadre de la lutte contre la fraude sociale, les indus et les erreurs. Elle n'est évidemment pas en mesure de calculer ce que les divers projets rapportent. Le cas échéant, chaque acteur individuel doit évaluer ce chiffre.