ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Compte rendu

Commission d'enquête relative à la lutte contre les fraudes aux prestations sociales

– Audition, ouverte à la presse, en visioconférence, de M. Frank Robben, administrateur général de la Banque Carrefour de la sécurité sociale belge 2

– Présences en réunion 12

Mardi
21 juillet 2020
Séance de 17 heures

Compte rendu n° 25

SESSION EXTRAORDINAIRE DE 2019-2020

Présidence de *M. Patrick Hetzel, président*

ASSEMBLÉE NATIONALE

**COMMISSION D'ENQUÊTE RELATIVE
A LA LUTTE CONTRE LES FRAUDES AUX PRESTATIONS SOCIALES**

Mardi 21 juillet 2020

La séance commence à dix-sept heures.

———

Présidence de M. Patrick Hetzel, président

La commission d'enquête relative à la lutte contre les fraudes aux prestations sociales procède à l'audition, ouverte à la presse, en visioconférence, de M. Frank Robben, administrateur général de la Banque Carrefour de la sécurité sociale belge.

M. le président Patrick Hetzel. Mes chers collègues, je tiens d'abord à vous informer que le rapporteur et moi-même nous sommes rendus vendredi dernier dans les locaux du service administratif national d'identification des assurés (SANDIA) à Tours, où nous avons été reçus par le directeur général de la Caisse nationale d'assurance vieillesse (CNAV), par la directrice des systèmes d'information, par le directeur des assurés de l'étranger, par la responsable du SANDIA et par plusieurs spécialistes des systèmes informatiques et des fichiers.

Nous étions accompagnés par deux responsables de la direction centrale de la police aux frontières (DCPAF) spécialistes de la détection de faux papiers et par un ancien collaborateur de la CNAV spécialisé dans la lutte contre les fraudes.

Ce déplacement nous a permis de mesurer l'ampleur des efforts déployés pour détecter et réprimer les fraudes, ainsi que les progrès accomplis ces dernières années. Il nous a également amenés à constater l'existence de points à améliorer, voire de failles, en matière d'accès à certains fichiers, de fiabilité de certaines informations ou de certains documents, de détection et de procédures.

Les documents de présentation qui ont accompagné cette visite ont été transmis à l'ensemble des membres de la commission d'enquête.

Nous sommes heureux d'accueillir, en téléconférence, M. Frank Robben, administrateur général de la Banque Carrefour de la sécurité sociale belge.

Monsieur, je vous remercie d'avoir répondu à notre invitation. Votre éclairage sera particulièrement précieux pour notre commission d'enquête car la structure que vous dirigez est très régulièrement citée en exemple, tant en France que dans d'autres pays européens.

Vous pourrez retracer l'histoire déjà longue de cet organisme créé en 1990, en nous indiquant ses réussites en matière de lutte contre la fraude, mais aussi en précisant quelles

sont les garanties qui encadrent votre activité en matière de protection des données, tant au niveau national qu'au niveau européen.

Nous serons également heureux de recueillir votre point de vue sur les dispositifs français de lutte contre la fraude, ainsi que sur les coopérations entre la Belgique et la France dans ce domaine.

L'article 6 de l'ordonnance du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires imposant aux personnes auditionnées par une commission d'enquête de prêter le serment de dire la vérité, toute la vérité, rien que la vérité, je vous invite à lever la main droite et à dire : « Je le jure. »

(M. Frank Robben prête serment).

M. Frank Robben, administrateur général de la Banque Carrefour de la sécurité sociale belge (BCSS). La Banque Carrefour de la sécurité sociale (BCSS) n'est pas une base de données centrale ; c'est un organisme public qui gère un réseau d'échanges d'informations entre 3 000 institutions environ en Belgique. Si l'une d'entre elles a besoin d'une information dont une autre dispose, la BCSS fait en sorte qu'elle ne soit pas demandée une seconde fois au citoyen ou à l'employeur concerné.

Nous avons également informatisé les informations qu'échangent les organismes de sécurité sociale avec les entreprises mais aussi, pour une large partie, avec les citoyens.

Le début et la fin de toute relation de travail doivent être déclarés par voie électronique – il n'est plus possible de le faire sur papier depuis 2004 –, dans le cadre de la déclaration immédiate de l'emploi dite Dimona. Nous avons aussi un système de déclaration trimestrielle des salaires et des temps de travail à destination de l'organisme qui perçoit les cotisations. Lorsqu'un autre organisme a besoin de ces informations pour calculer les allocations, c'est auprès de lui qu'il va les chercher.

La BCSS est donc un pivot qui organise tous ces échanges d'informations. À sa création en 1990, 800 formulaires papier étaient échangés en moyenne chaque année entre citoyens, entreprises et institutions de sécurité sociale ; ils ont été remplacés par 220 flux électroniques. Nous avons ainsi supprimé les trois quarts des formalités administratives, et tout se fait par voie électronique.

Ce n'est pas une base de données centralisée ; chaque institution de sécurité sociale dispose de ses propres données, mais les autres peuvent y avoir accès lorsqu'elles en ont besoin.

Nous avons créé en 1990 un comité de sécurité de l'information (CSI), nommé par le Parlement, qui est chargé d'autoriser au préalable tout échange de données personnelles. Un organisme de sécurité sociale ayant obtenu légitimement des informations à caractère personnel peut, moyennant l'autorisation de ce comité, les mettre à la disposition d'un autre organisme qui en aurait besoin. Cela permet de s'assurer que cet échange est légitime, proportionnel – afin de ne pas donner plus d'informations que nécessaire – et sécurisé.

Ainsi, 1,2 milliard d'informations sont échangées chaque année entre ces 3 000 institutions. Ce sont les organismes classiques de sécurité sociale, publics ou privés – mutualités ou caisses d'allocations chômage –, qui perçoivent les cotisations ou calculent et paient les allocations de chômage, les indemnités pour accident de travail, maladie

professionnelle ou incapacité de travail, les pensions de retraite et les allocations familiales ; mais aussi les systèmes d'aides sociales, comme le revenu d'intégration et les allocations aux personnes handicapées, ainsi que toutes les institutions qui donnent des avantages sur la base du statut social – firmes de transport public, gaz, électricité, eau, télécommunications –, et services fiscaux qui donnent des réductions de taxes. Toutes sont connectées à ce réseau.

En Belgique, une personne bénéficiant d'allocations pour personne handicapée recevait il y a trente ans une dizaine de formulaires papier afin de demander à diverses institutions le tarif social auquel elle avait droit ; aujourd'hui, son statut social est envoyé avec son accord à sa firme de gaz, d'électricité ou d'eau, et ces droits lui sont attribués automatiquement.

Sur le plan de la lutte contre la fraude, tout le monde est identifié par un numéro unique dans l'ensemble des bases de données. Avant d'attribuer des allocations, chaque institution peut d'abord contrôler la situation du demandeur pour déterminer s'il y a bien droit, par exemple en vérifiant que quelqu'un qui demande des allocations chômage ne travaille pas. Les différents services d'inspection sociale collaborent en travaillant sur une plateforme commune qui leur permet de se répartir le travail, ce qui n'était pas le cas il y a vingt ans ; ils ont également accès à une plateforme de coopération dédiée aux procès-verbaux. Par ailleurs, un système d'exploration de données (*datamining*) permet de rassembler des informations pseudonymisées à des fins de vérification ; quand une fraude est constatée, on peut identifier la personne et prendre les mesures qui s'imposent.

Nous pouvons donc nous appuyer sur un large système de *data warehousing*, entrepôt de données dans lequel les informations sont mises en relation et facilement visualisables. Ainsi, il y a quelques années, lorsqu'un dispositif a été instauré afin de diminuer certains coûts pour les entreprises nouvellement créées, nous avons pu automatiquement détecter celles qui fermaient pour être refondées sous une autre forme – par exemple en continuant à employer les mêmes salariés, en travaillant avec les mêmes sous-traitants et en étant domiciliées à la même adresse. Avec ce système, nous avons gagné sur trois plans : la fraude est détectée beaucoup plus rapidement qu'avant, en moyenne un trimestre plus tôt ; nous sommes capables de traiter des cas beaucoup plus complexes ; enfin, nous sommes plus efficaces, puisque ces outils nous permettent d'obtenir en une heure les résultats que nous obtenions auparavant en une journée. Grâce aux techniques de *datamining*, nous pouvons interconnecter de manière temporaire des informations provenant de plusieurs bases de données, sur la base du numéro unique, et ensuite les utiliser pour lutter contre la fraude.

M. Pascal Brindeau, rapporteur. L'efficacité de la BCSS réside dans la conjonction de deux éléments. Grâce au *datamining*, on peut croiser les données d'un maximum d'organismes publics intervenant dans le champ des prestations sociales. De ces échanges de données naît une meilleure connaissance de la situation de toute personne prétendant à un certain nombre de droits ; couplés au numéro d'authentification unique propre à chaque individu, ils permettent aux organismes concernés de contrôler a priori l'état des droits à prestation.

Depuis 2014, l'équivalent de la carte Vitale belge a été intégré dans une carte d'identité électronique (eID). Quelles en sont les caractéristiques ? Est-elle biométrique ou protégée d'une quelconque manière, puce électronique ou cryptage ?

M. Frank Robben. L'eID n'est pas biométrique ; c'est une carte à puce intelligente dotée d'un microprocesseur, et non une carte mémoire. Elle a trois fonctions : identifier une

personne, authentifier son identité, et générer une signature électronique juridiquement valable.

L'identification se fait sur la base d'un certain nombre de données comme le numéro unique, le nom et le prénom. On peut utiliser la carte par exemple pour s'authentifier afin d'accéder à un site web, donc pour prouver que l'on est bien la personne que l'on prétend être, mais aussi pour signer numériquement un document. On y trouve uniquement des données d'identité. Je suis opposé à ce qu'elle comporte du contenu qui serait susceptible de changer, car il faudrait alors la mettre à jour régulièrement, et, en cas de perte, toutes ces informations risqueraient d'être perdues. Une copie des données pourrait certes être accessible ailleurs, mais il ne serait alors pas nécessaire qu'elles se trouvent sur la carte elle-même.

Cette carte ne comporte donc pas de statut d'assurabilité, ni de données médicales. La carte d'identité électronique a remplacé en 2000-2001 la carte de sécurité sociale – ou carte SIS, pour système information sociale –, qui était une carte à mémoire et non à microprocesseur ; elle contenait des données d'assurabilité et de soins en plus de celles permettant l'identification. Depuis que nous disposons d'un réseau internet auquel tout le monde peut se connecter, nous avons cessé d'y mettre des informations de contenu, car celles-ci sont disponibles dans des bases de données. Une carte aux données stables constitue le système optimal. En matière de protection des données, c'est également la meilleure solution car l'accès aux autres informations, qui doit être autorisé au préalable par un comité indépendant, est mieux contrôlé que sur une carte où elles pourraient être lues de manière décentralisée par plusieurs personnes.

M. Pascal Brindeau, rapporteur. Lors de la mise en place de cette carte d'identité électronique, avez-vous eu un débat sur la biométrie ? Compte tenu de ses caractéristiques – une carte à puce qui permet la lecture de données, l'authentification de l'identité et une signature électronique –, quel est son niveau de protection ? Avez-vous à faire face, comme c'est le cas en France pour un certain nombre de documents, à une délinquance liée à la fraude à l'identité, donc à des problématiques d'usurpation d'identité ? Chez nous, elle s'est fortement développée à travers des chaînes de falsification qui parviennent à pénétrer des systèmes pourtant sécurisés.

M. Frank Robben. La carte d'identité électronique existe depuis 2001 en Belgique ; je l'ai élaborée en collaboration avec d'autres personnes et je pourrais vous expliquer tout le système cryptographique qui sous-tend son fonctionnement. Nous n'avons jamais eu de problèmes de sécurité liés à la carte elle-même et nous n'avons jamais rencontré de carte falsifiée. Il n'est pas non plus possible de copier les informations d'une carte sur une autre sans que le système le détecte au moment de la lecture, car chaque puce dispose d'un microprocesseur assorti d'un numéro de châssis unique, utilisé comme paramètre dans le cryptage de données. Elle est donc parfaitement protégée.

La biométrie est un instrument d'authentification. S'identifier, c'est répondre à la question : « Qui êtes-vous ? » ; s'authentifier, c'est répondre à une question différente : « Prouvez-moi que vous êtes la personne que vous prétendez être. » On peut s'authentifier de trois façons – ou par la combinaison de ces trois façons : soit par un objet que l'on possède, soit par une information que l'on connaît, soit par ce que l'on est. La carte d'identité électronique belge combine pour le moment les deux premiers critères : il faut détenir physiquement la carte et connaître son code PIN. Dans les nouvelles cartes qui sont distribuées depuis quelques mois, la puce contient aussi l'empreinte digitale. Pour prouver son identité, il faut mettre son doigt sur un lecteur qui est coordonné localement avec le contenu

de la puce, ce qui permet de comparer les deux. Il ne s'agit que d'une preuve locale : comme l'a préconisé l'organisme belge comparable à votre commission nationale de l'informatique et des libertés (CNIL), il n'y a pas de base de données centralisée qui stockerait toutes les empreintes digitales. Nous n'avions pas intégré ce dispositif en 2001 parce qu'il n'existait alors pas de standard suffisant en la matière ; il y avait beaucoup de faux positifs et de faux négatifs. Depuis, le système est devenu beaucoup plus sûr, ce qui nous a permis de commencer à utiliser la biométrie il y a quelques mois ; elle est d'ailleurs imposée par l'Union européenne pour un certain nombre de documents.

Je l'ai dit, l'usurpation d'identité ne peut se faire en copiant une carte. Il est toujours possible que quelqu'un parvienne à intégrer les bases de données – notamment le registre national – et à obtenir une carte sans que l'on ait bien vérifié qu'il est effectivement celui qu'il prétend être avant de la lui donner, mais cela n'a rien à voir avec l'informatique. Les procédures qui précèdent l'attribution d'une carte doivent être suffisamment sécurisées pour garantir que personne ne dispose de deux identités.

M. le président Patrick Hetzel. Réalisez-vous une estimation de la fraude sociale en Belgique ? Plus précisément, disposez-vous d'une estimation des fraudes liées aux risques couverts par la sécurité sociale belge, qu'il s'agisse de l'assurance maladie, vieillesse ou famille ?

M. Frank Robben. Il m'est difficile de répondre à cette question, car je ne suis pas un inspecteur social, ni le représentant d'un organisme luttant contre la fraude. La BCSS se contente de faire en sorte que tout le monde sache utiliser les outils à disposition pour lutter contre la fraude.

Nous disposons, je l'ai dit, d'un système de déclaration multifonctionnel qui nous permet de recevoir tous les trois mois des informations sur le salaire et le temps de travail des gens. Auparavant, chaque fois qu'un organisme de sécurité sociale avait besoin d'une de ces informations – en particulier l'office national de la sécurité sociale (ONSS), pour calculer les cotisations dues –, il devait la demander directement à l'employeur, qui pouvait tout à fait omettre de déclarer certains éléments du salaire versé à ses employés – primes de fin d'année, chèques repas par exemple –, tout en les déclarant s'agissant d'employés tombés malades ou ayant subi un accident de travail. C'était une manière de frauder. Or il n'est désormais plus possible de transmettre des informations différentes selon les situations, car celles qui sont contenues dans la déclaration faite à l'ONSS sont automatiquement utilisées pour calculer le montant d'une allocation. Les éléments non déclarés du salaire n'étant pas pris en compte, les syndicats s'opposent à une telle pratique dont pâtissent les salariés en cas de problème.

Des garanties contre la fraude existent donc. Dans les années 1990, quand un salarié payait des cotisations sociales, il recevait un bon de cotisation qu'il devait envoyer à sa mutuelle pour prouver qu'il en versait suffisamment. Certaines personnes faisaient une copie de ce bon et le transmettaient à plusieurs mutuelles ; elles allaient chez le médecin, payaient la consultation et copiaient la feuille de soins pour être remboursées parfois cinq ou six fois. Ce n'est plus possible grâce à un répertoire de référence qui nous permet de savoir précisément qui dispose d'un dossier dans quelle institution de sécurité sociale ; on ne peut y être affilié à plusieurs mutualités. Lorsqu'il a été créé, nous nous sommes rendu compte qu'une personne était affiliée – par des formulaires papier – à quinze ou seize mutuelles différentes, qui lui remboursaient toutes chaque prestation.

Ces exemples témoignent des garanties qui émanent automatiquement du système lui-même. En outre, lorsque l'on calcule le montant d'une allocation de sécurité sociale, on a désormais accès à l'ensemble des informations concernant les allocations touchées par la personne concernée. Les cumuls d'allocations non autorisés ne sont plus possibles, car ils sont directement repérés. Je peux donc vous parler des fraudes évitées, mais il m'est difficile de me prononcer sur celles qui continuent à être pratiquées.

Le bureau fédéral du plan (BFP), organisme indépendant chargé notamment de réaliser des prévisions macro-économiques, avait calculé il y a une dizaine d'années que l'action de la BCSS permettait d'économiser 1,7 milliard d'euros chaque année ; ces avantages financiers étaient liés à la diminution des charges sociales et administratives pour les entreprises et les citoyens, mais aussi, pour partie, à la lutte contre la fraude.

Je gère le système d'échanges d'informations belge non seulement dans le secteur social, mais aussi dans celui de la santé, à travers la plateforme eHealth qui met en relation notamment les médecins, les hôpitaux et les laboratoires, les cliniques. Il ne s'agit pas de lutte contre la fraude, mais nous obtenons là aussi des gains importants. Environ un quart des citoyens belges ont une maladie chronique ; éviter par exemple une analyse de sang par an et par patient chronique – car souvent les mêmes examens sont réalisés deux fois, ce qui n'a aucun sens – permet d'épargner 250 millions d'euros. La BCSS coûte entre 14 et 15 millions d'euros par an, et la plateforme eHealth environ 12 millions d'euros par an ; elles représentent des retours sur investissement qui sont loin d'être négligeables.

M. le président Patrick Hetzel. En tant qu'expert ayant œuvré à la mise en place d'un système efficace, fruit d'un énorme travail en Belgique, quel regard portez-vous sur la politique française de lutte contre la fraude aux prestations et aux cotisations sociales, qui reste pour le moins perfectible ?

M. Frank Robben. Je n'ai pas pu étudier en détail le système français. Le modèle de la BCSS permet de conserver un stockage et un traitement des données qui soient décentralisés, tout en laissant la possibilité de les mettre en forme et de les échanger lorsque c'est nécessaire, que ce soit pour simplifier la vie des gens ou pour lutter contre la fraude. Nous avons eu ce débat il y a trente ans en Belgique : la protection de la vie privée constitue parfois un argument facile pour ne pas avoir à débattre de l'existence même de chaque institution. En Belgique, il y a un nombre important d'institutions de sécurité sociale ; elles veulent naturellement continuer à exister. Il n'est pas facile de les rendre dépendantes d'une base de données centrale, car elles se sentent menacées de disparition.

Notre système a le mérite de n'être pas trop intrusif ; tout en évitant de centraliser les informations et de les rendre trop dépendantes les unes des autres, il permet de les mettre à disposition, de les rassembler et de les échanger si besoin. Pour vérifier qu'une personne prétendant avoir droit à une allocation de chômage ne travaille pas, il n'est pas nécessaire de centraliser ou de copier les données sur l'emploi ; il suffit de les consulter lorsque c'est nécessaire auprès de l'institution détenant l'information recherchée, en disposant d'un numéro unique d'identification permettant de s'assurer qu'il s'agit bien de la même personne. Beaucoup disent qu'un tel numéro constitue une atteinte à la vie privée, mais nous l'avons conservé car seul le croisement des données peut être dangereux.

Avec la BCSS, nous avons créé un endroit central par lequel doivent passer tous les échanges d'informations, mais qui ne peut se voir confier de missions de contenu – calcul de cotisations ou attribution d'allocations ; elle doit être une « *clearing house* », c'est-à-dire une

tierce partie de confiance qui contrôle le fait que telle ou telle donnée puisse être échangée, l'autorisation étant donnée par le CSI. L'enjeu n'est pas l'existence d'un numéro unique ; je peux vous retrouver tout de suite dans les bases de données même si je ne dispose pas du vôtre, grâce au couplage de données permis par les outils d'intelligence artificielle. Ce qui est important, c'est d'apporter des garanties en contrôlant l'échange d'informations et en déterminant dans quels cas il est légitime. C'est pourquoi on ne peut le faire que lorsque c'est autorisé par la réglementation, soit pour attribuer automatiquement des droits, soit pour diminuer les charges administratives, soit pour lutter contre la fraude.

M. le président Patrick Hetzel. La BCSS est-elle aussi utilisée dans le cadre de la lutte contre les fraudes transfrontalières ?

Recevez-vous des données des partenaires français ou leur en envoyez-vous ?

M. Frank Robben. Il existe au niveau européen le réseau d'échange électronique d'informations sur la sécurité sociale (EESSI), entre les institutions de sécurité sociale des différents États membres de l'Union européenne. Pour la Belgique, toutes les demandes d'information émanant de ce réseau sont envoyées à la BCSS ; nous les transmettons à l'institution concernée, puis nous renvoyons la réponse.

Le modèle d'un tel réseau a été élaboré dès 1993. Les différents pays européens rencontrent en partie les mêmes problèmes : comment sait-on que l'on parle de la même personne ? Comment identifie-t-on l'institution compétente ? En Belgique, s'agissant des pensions de retraite, c'est le statut professionnel de chacun qui détermine quel organisme est compétent ; nous en avons un pour les travailleurs indépendants, un autre pour les travailleurs salariés, et un autre pour les fonctionnaires. Chez vous, le système est organisé de façon beaucoup plus territoriale ; il faut connaître les critères pour pouvoir s'adresser à la bonne institution.

La BCSS tient par ailleurs un registre des liens, qui fait le lien entre le numéro unique belge de chaque personne – qu'elle soit belge ou pas – et son identifiant étranger. Lorsqu'une demande d'information nous est adressée, nous sommes en mesure de passer de l'un à l'autre ; nous traitons cette affaire en Belgique à partir du numéro belge, puis la réponse est envoyée avec l'identifiant d'origine, par exemple français. Nous coopérons donc sur ce plan, mais il faut avouer qu'au niveau européen, l'échange de données n'est pas toujours évident ; on ne sait pas forcément quel est l'organisme compétent auquel s'adresser, ni, dans l'autre sens, si l'organisme demandeur a le droit d'obtenir les informations qu'il requiert. Par ailleurs, nous ne disposons pas toujours des mêmes systèmes de cryptage pour sécuriser les données. La Commission européenne devrait mettre à disposition davantage de services de base pour que nous progressions dans ce domaine ; nous avions d'ailleurs écrit il y a quelques années un rapport consacré à l'échange d'informations à l'échelle internationale.

M. Pascal Brindeau, rapporteur. La plateforme de la BCSS ne stocke donc pas les données personnelles collectées par les différents organismes qui y participent, ce qui lui permet de répondre aux prescriptions du règlement général sur la protection des données (RGPD) européen. Il n'y a pas de fichier centralisé et les informations demeurent au niveau de chaque organisme de prestation, mais il est possible à tout moment de les consulter pour déterminer si une personne a droit ou pas à telle ou telle prestation. Sur requête, vous pouvez vérifier l'identité d'une personne, sa situation d'emploi – ou d'absence d'emploi – et les droits qui y sont associés, mais aussi sa situation familiale – est-elle mariée, en union libre, isolée ? – et de logement. Est-ce bien cela ?

M. Frank Robben. La Banque Carrefour elle-même, qui comprend 80 personnes – surtout des informaticiens –, n'a accès à aucune information. Elle organise les échanges d'informations dans le respect des autorisations données par le comité indépendant, qui est nommé par le Parlement et dont l'intervention est obligatoire. Le CSI est composé de deux types de spécialistes, les uns en protection des données et de la vie privée, les autres en sécurité sociale et en protection sociale.

Par exemple, un organisme qui calcule des allocations familiales a-t-il besoin de savoir si un des deux parents de l'enfant est un chômeur de longue durée ? Pour répondre à cette question, il faut déterminer si une majoration existe dans ce cas précis, donc connaître le droit social ; un spécialiste en protection des données ne peut pas le faire. C'est le CSI, sous contrôle parlementaire – il s'agit de droits fondamentaux –, qui est chargé de trouver cet équilibre entre le droit constitutionnel à la protection sociale d'une part, à la protection des données d'autre part, pour autoriser ou non l'échange de données. La BCSS intervient ensuite : en fonction de la décision prise par le comité, elle donne ou elle refuse l'accès à l'information, par exemple à la caisse d'allocations familiales qui a sollicité une caisse d'allocations chômage à propos de la situation d'emploi d'un père de famille. Au préalable, on a vérifié que son enfant est bien affilié à l'organisme qui fait la demande ; un autre ne pourra pas obtenir satisfaction. Si une mutuelle a besoin de connaître mon adresse, seule celle à laquelle je suis adhérent – et aucune autre – peut accéder à cette information.

Les règles concernant l'échange de données sont déterminées par le CSI ; la BCSS, tierce partie de confiance, s'assure qu'elles sont respectées mais n'utilise aucune information. Nous n'attribuons pas de droits, nous ne faisons pas de calculs de cotisations, et nous n'organisons pas la lutte contre la fraude – c'est le rôle par exemple des inspecteurs sociaux.

M. le président Patrick Hetzel. Quels sont les rapports entre le CSI et l'autorité de protection des données (APD), équivalent belge de la CNIL ?

M. Frank Robben. L'APD a la même mission que la CNIL : donner des avis, faire des contrôles, sanctionner. Elle peut contrôler toutes les institutions de sécurité sociale, ainsi que la BCSS. Le CSI, lui, est un comité dont les décisions ont une portée normative sur le plan juridique : il indique dans quelle situation des données peuvent être échangées, à quelles fins et entre quels acteurs. À condition qu'elles ne s'opposent pas à une norme plus élevée comme le RGPD, ses autorisations donnent une base légale aux organismes de sécurité sociale lorsqu'ils échangent des informations.

Prenons le cas de deux organismes – A et B – qui disposent tous les deux d'une base juridique – le RGPD – pour traiter de l'information. S'ils ont besoin de la même information, le rôle du CSI est par exemple d'autoriser l'organisme A à la transmettre à l'organisme B. Il s'agit d'une mesure de protection des données qui va beaucoup plus loin que le RGPD ; elle permet d'effectuer un contrôle en amont pour agir de manière proportionnelle et sécurisée.

Le CSI a donc un pouvoir normatif, alors que l'APD a une mission d'avis, de contrôle et de sanction. Le RGPD décrit d'ailleurs clairement ce qu'une autorité de protection des données peut faire ou ne pas faire. Avant son entrée en vigueur, un certain nombre de membres de l'APD siégeaient au CSI ; ce n'est plus autorisé, et nous avons scindé clairement les deux institutions.

M. Alain Ramadier. Vous avez dit que le numéro unique dépendait de la carte d'identité électronique, apparemment infalsifiable. Pouvez-vous le confirmer ? Cela sous-

entend que tout le monde en Belgique dispose d'une carte d'identité, et que celle-ci est nécessaire pour accéder aux différentes caisses.

Dépendez-vous d'un ministère ? Êtes-vous contrôlés, avez-vous un rapport annuel à rendre à un ministère de tutelle ou aux parlementaires, comme nous le faisons en France ?

Le fonctionnement du système belge suscite l'admiration : tout le monde va dans le même sens et partage les données, ce qui loin d'être le cas en France où l'on travaille davantage en silo. En combien de temps avez-vous élaboré ce dispositif, et quel est le coût de son fonctionnement annuel ?

M. Frank Robben. La BCSS coûte entre 14 et 15 millions d'euros par an. J'ai fait des études de droit et d'informatique ; sa conception était le sujet de mon mémoire de fin d'études, pour lequel j'ai reçu un prix scientifique. On m'a alors demandé de la créer ; nous avons commencé en 1986 – j'ai installé moi-même le premier programme –, et le système était opérationnel en 1990-1991. Nous avons ensuite progressivement simplifié toutes les procédures, et les principaux éléments de la structure actuelle étaient prêts en 2002-2003. Il a donc fallu une quinzaine d'années pour tout mettre en place. Depuis vingt ans, on m'a régulièrement confié de nouvelles missions pour appliquer ce modèle dans d'autres domaines : j'ai créé un système comparable pour l'État fédéral, pour le secteur de la santé, et je suis en train de le faire pour la justice ; je m'occupe également du suivi des contacts dans le cadre de la crise du coronavirus.

La carte contient le numéro unique qui permet au porteur de prouver son identité, mais ce n'est pas parce que l'on n'a pas la carte sur soi que l'on ne peut y accéder – nous ne voulons pas d'un fossé digital. Les enfants de moins de douze ans ont une carte en plastique sans puce ; à partir de douze ans, la carte d'identité électronique est obligatoire et tout le monde en dispose. Le numéro unique, lui, est créé juste après la naissance ; il est d'emblée utilisé comme clé d'identification.

J'ai eu la chance d'être sollicité pour créer ce système à 24 ans, et on m'a nommé administrateur général de l'institution à 29 ans. On s'est jeté à l'eau, et le travail s'est effectué en coopération avec l'ensemble des instances concernées. De tels changements nécessitent d'instaurer un climat de confiance, dans lequel le projet est mené à bien de manière collective. Ainsi, eHealth, dont personne ne voulait se servir à l'origine dans le domaine de la santé, voit s'échanger 17 milliards de données après dix ans d'existence. Il faut que le système soit transparent quant à ses attributions, et qu'il fasse l'objet d'un contrôle étroit en matière de sécurité de l'information – c'est à cela que servent le CSI et l'APD. Ses avantages doivent par ailleurs apparaître clairement : il est compréhensible que les gens ne veuillent pas donner plusieurs fois la même information à différentes institutions de sécurité sociale, ou qu'un patient qui a subi un jour un choc allergique vis-à-vis d'un médicament souhaite éviter qu'un autre médecin lui prescrive le même type de médicament cinq ans plus tard. Pour cela, il faut échanger de l'information, et le faire de manière pertinente.

La BCSS et eHealth sont gérés par les représentants des personnes sur qui on échange de l'information. C'est selon moi un élément crucial. Il est impossible de mettre en œuvre un tel projet en un ou deux ans ; cela nécessite de la continuité, donc de n'être pas trop lié à la situation politique d'un moment donné. J'ai travaillé pour des ministres libéraux, socialistes ou chrétiens démocrates, flamands ou wallons… Le comité de gestion de la Banque Carrefour ne dépend donc pas directement d'un ministère ; il est composé de représentants des travailleurs salariés et des travailleurs indépendants – les syndicats –, des entreprises et des

organismes de sécurité sociale. Ce sont eux qui déterminent nos priorités, ce que l'on fait et comment on le fait. C'est la même chose dans le secteur de l'e-santé ; c'est une autre institution, mais elle est pareillement gérée par les représentants des médecins, des hôpitaux, des kinésithérapeutes, des pharmaciens, des mutuelles et des institutions publiques de santé. Ces deux organismes sont contrôlés de façon structurelle et font l'objet d'une évaluation régulière ; je suis moi-même évalué chaque année par les clients – ceux sur qui on échange de l'information –, ce qui constitue une forme de garantie.

Nous sommes une plateforme informatique ; nous ne produisons plus de rapports annuels sur papier, mais nous tenons à jour en permanence le fonctionnement de notre institution sur un site web très étendu, qui décrit de manière très détaillée tous les échanges d'informations – plus de 15 000 pages de documentation sont disponibles à ce propos.

M. le président Patrick Hetzel. Votre site est en effet très bien documenté. Le rapport parlementaire réalisé l'année dernière par la sénatrice Nathalie Goulet et la députée Carole Grandjean avait indiqué que la BCSS belge était un bel exemple de lutte contre la fraude – elle a en outre lancé la Banque Carrefour des entreprises qui lui permet d'être encore plus efficace –, tout en étant un service de qualité permettant de faciliter à la fois la vie des assurés en limitant leurs démarches administratives, et le travail des organismes de sécurité sociale qui peuvent effectuer des requêtes sur une base de données consolidée.

Je vous remercie de votre contribution ; nous ne manquerons pas de citer votre exemple, dont nous espérons qu'il pourra inspirer les responsables français en la matière.

L'audition s'achève à dix-huit heures cinq

Membres présents ou excusés

Commission d'enquête relative à la lutte contre les fraudes aux prestations sociales

Réunion du mardi 21 juillet 2020 à 17 heures

Présents. - M. Pascal Brindeau, M. Patrick Hetzel, M. Alain Ramadier

Excusés. - Mme Josette Manin, M. Thomas Mesnier