Garantir la confidentialité des fichiers détenus par les statisticiens et chercheurs en sciences sociales

Claude POULAIN
RSSI de l'Insee de 1995 à 2005
8, rue des 4 chemins, 63117-Chauriat
cfg.poulain@wanadoo.fr

Résumé : Les organismes qui détiennent des fichiers de données sur les personnes affirment que la loi Informatique et libertés est respectée, notamment que la confidentialité est assurée. Pourtant, que ce soit pour des raisons économiques ou culturelles, les raisons d'en douter sont nombreuses. De ce fait, face aux affirmations des organismes, les personnes fichées ou leurs représentants, conservent leurs doutes, les uns et les autres campant sur leurs positions.

Pour sortir de cette situation il est proposé de faire appel à un organisme tiers capable d'expertiser la réalité des mesures de sécurité annoncées et d'en rendre compte.

Une telle solution s'inspire de ce qui existe pour valider auprès des actionnaires la comptabilité de leur entreprise : pour sortir de l'affirmation de l'une et de la suspicion des autres, c'est un commissaire aux comptes, extérieur aux deux parties, qui est chargé d'examiner l'exactitude et la sincérité de la comptabilité et d'en informer l'assemblée générale. Le même mécanisme est utilisé pour la certification « qualité » des entreprises : pour revendiquer auprès de leurs clients les labels de qualité ISO 9000, les entreprises se font examiner par des organismes de certification.

Mots clés : données personnelles**,** confidentialité, audit, sécurité.

Summary: The organizations which hold data files on people assert that the law « Informatique et libertés » (Computing and freedoms) is respected, and in particular that confidentiality is assured. However, whether it is for economic or cultural reasons, there are many reasons for doubting it. Therefore, despite the assertions of the organization, filed people and their representatives keep doubting, and each party stands its ground.

To get out of this situation it is suggested to call upon a third organization able to appraise the reality of the announced security measures and to give an account of it.

Such a solution is inspired by the existing system for validating the accountancy of their company to shareholders: in order to go beyond the assertions of the formers and the suspicion the latters, it is an auditor, external to the two parties, who is in charge of examining the accuracy and the sincerity of the accountancy and of informing the general assembly of it. The same mechanism is used for "quality certification" of the companies: to assert their quality control marks ISO 9000 to their customers, the companies get themselves assessed by certification organizations.

Key words: personal data, confidentiality, audit, safety.

1- Position du problème

En 2006, lors d'une séance du Conseil National de l'Information Statistique, un consortium d'organismes de recherche a proposé un projet « d'Etude Longitudinale Française depuis l'Enfance » (ELFE) consistant à construire un panel de 20.000 personnes à suivre depuis leur naissance jusqu'à leur âge adulte, voire jusqu'à leur décès en rassemblant sur elles un maximum d'informations sanitaires, environnementales, familiales, sociales, scolaires, professionnelles, …

Ce Conseil National de l'Information Statistique est un organisme consultatif chargé d'examiner les programmes statistiques et de donner son avis sur les projets d'enquêtes menées par les organismes publics ou para-publics. Il est composé d'une centaine de membres dont des représentants des Assemblées, des syndicats, des associations, de l'Administration, etc. Il est structuré en commissions spécialisées et c'est à une « inter-formation » sur les statistiques sociales que ce projet ELFE a été présenté.

Il l'a été par un chercheur de l'Ined au nom d'un Groupement d'Intérêt Scientifique (GIS) rassemblant, outre l'Ined[1], l'Inserm, l'Insee, l'InVS, trois directions ministérielles, la DGS et la Drees du ministère de la Santé enfin la DEPP du ministère de l'Education.

Les éléments repris ici sont extraits du compte-rendu de cette réunion tel qu'il est disponible sur le site Internet du CNIS[2].

L'alimentation de la base de données de ces 20.000 personnes se fera par enquêtes et, chaque fois que possible, par la récupération d'informations provenant de l'Insee, des CAF, des enquêtes de santé scolaire, …La première enquête, en maternité, est prévue pour 2009. Cette cohorte sera à la disposition des chercheurs*, « une trentaine d'équipes en sciences sociales et une trentaine en santé ont été sollicitées, 90 projets, dans différentes disciplines étant déjà sur les rangs[3] ».*

Comme le disait un auditeur cité dans le compte-rendu : « *je ne peux me garder d'un mouvement de recul devant la somme des données qui seront collectées sur un individu dès la naissance ».*

Il faut noter qu'il s'agit ici d'une cohorte. Dans une enquête ponctuelle, une fois la collecte réalisée, il est possible d'effacer les principaux éléments d'identification comme le nom et l'adresse[4]. Avec une cohorte il n'est pas possible de les effacer : pour que l'on puisse, d'année en année et pour le même individu, ajouter l'information trouvée dans les fichiers de

---

[1] Ined :Institut National d'Etudes Démographiques, qui abrite un site dédié à ce projet : https://www.elfe.ined.fr/
Inserm : Institut National de la Santé et de la Recherche Médicale,
Insee : Institut National de la Statistique et des Etudes Economiques,
InVS : Institut National de Veille Sanitaire,
DGS : Direction Générale de la Santé,
DREES : Direction de la Recherche, des Etudes, de l'Evaluation et des Statistiques (service statistique ministériel des ministères en charge de la santé et de la protection sociale),
DEPP : Direction de l'Evaluation, de la Prospective et de la Performance du ministère de l'Education nationale.

[2] Voir : http://www.cnis.fr/ind_doc.htm, page 25 à 28 du compte-rendu. Rédigés avec soin et révisés par les participants, ces comptes-rendus peuvent être considérés comme fiables.

[3] Rapport cité p. 26.

[4] La CNIL oblige d'ailleurs à procéder à un tel effacement.

l'administration, des organismes sociaux ou collectée directement par voie d'enquête, il est indispensable de disposer de tous les éléments possibles d'identification : nom, prénom, date de naissance, l'adresse ou les adresses successives, numéro de sécurité sociale, identifiant élève, numéro d'allocataire de la CAF, etc.

Les concepteurs du projet n'ignorent évidemment pas les problèmes posés en matière de respect de la vie privée. Voici ce que l'on peut lire dans le compte-rendu de la séance du CNIS :

« Cette accumulation de données pose des problèmes de protection des personnes, auxquels nous réfléchissons beaucoup. Un groupe spécifique sera constitué sur les questions d'informatique et de protection des données et aura pour charge d'explorer toutes les possibilités offertes par les nouvelles techniques d'anonymisation. Nous sommes en contact avec la CNIL sur ce point depuis déjà un an. De même, un groupe d'éthique sera probablement mis en place rapidement, afin d'étudier les questions qu'il sera possible de poser aux ménages et la manière de les informer. Enfin, les instances de contrôle seront consultées, le Cnis, la CNIL ainsi que le Comité de protection des personnes pour les recherches en biologie (CPPRB) s'il y a des prélèvements biologiques [5]».

A une question sur la dangerosité du projet, il est répondu :

« Les méthodes d'anonymisation ne répondent qu'à une partie du problème, la question de l'identification indirecte par les caractéristiques des personnes se posant également. A cet égard, il n'est pas imaginable que la base de données constituée soit ouverte sans précaution à l'ensemble des chercheurs. Nous voulons certes une politique d'ouverture à la communauté scientifique, mais il convient de mettre en place des systèmes, et nous sommes demandeurs de conseils en la matière et de guides de la part d'instances comme le Cnis[6] ».

Et, plus loin :

« Des techniques perfectionnées, agréées par la CNIL, existent désormais, qui offriront toute satisfaction aux statisticiens et aux responsables de l'opération[7] ».

A la fin, le président de l'inter-formation statistiques sociales du CNIS peut conclure la consultation :

« Sous ces précautions, il n'y a pas d'objections ? L'interformation [du CNIS] rend un avis d'opportunité favorable ».

Cet exemple est intéressant en ce qu'il rassemble la plupart des arguments habituellement utilisés dans les projets présentant des exigences de confidentialité[8].

---

[5] Ibid. p.26.
[6] Ibid. p.27.
[7] En effet, ce que redoutent les chercheurs c'est que le respect des règles de sécurité alourdisse leur travail quotidien. Il faut donc trouver un compromis entre la protection de la confidentialité et la facilité d'accès pour les chercheurs.
[8] D'autres projets de même nature existent. Quelques mois auparavant, l'Insee avait présenté devant le même CNIS un projet de panel de population (dit échantillon démographique permanent EDP++) qui, s'il devait contenir moins de données sur chaque individu, portera sur une population de 2 à 3 millions de personnes, soit près du vingtième de la population (le texte d'extension a été pris JO du 16 janvier 2007) .

1.1- Invocation du caractère scientifique de la demande

Le projet provient d'organismes scientifiques réputés : l'Ined, l'Inserm, l'Insee, l'InVS… Il est préparé par un Conseil scientifique d'une quinzaine d'experts français et étrangers.

Il s'agit en effet de ne pas confondre un tel projet avec ceux qui peuvent être proposés par des entreprises, par le fisc ou par le ministère de l'intérieur. Les objectifs sont ici « désintéressés » ; il n'y a rien à vendre ni rien à contrôler. Ils visent à l'amélioration des connaissances. Cette particularité est tout à fait utile pour susciter la confiance d'organismes comme le Cnis ou la CNIL mais aussi celle des personnes que l'on va interroger. La CNIL notamment s'est vue critiquée, dès la mise en place de la loi de 1978, comme mettant trop d'entraves à la recherche scientifique en France. De ce fait, lors de la ré-écriture de la loi en 2004, des dispositions plus favorables aux chercheurs ont été introduites et il est clair que la CNIL leur autorise des projets ou des pratiques qu'elle interdirait aux autres.

1.2- La plus grande attention est apportée aux questions de confidentialité

« Nous réfléchissons beaucoup aux problèmes de protection des personnes »… « Il n'est pas imaginable que la base de données constituée soit ouverte sans précaution à l'ensemble des chercheurs ».

Ces organismes connaissent l'existence de la loi Informatique et libertés. Depuis 1978, leurs services juridiques sont parvenus à convaincre les chercheurs et surtout leurs directions qu'il était dans leur intérêt de la respecter. Lorsque leurs enquêteurs vont se présenter dans les familles, il sera bienvenu de pouvoir dire que la CNIL a donné son accord et que la confidentialité est donc, en principe, garantie.

« Nous sommes en contact avec la CNIL sur ce point depuis déjà un an. »… « Les instances de contrôle seront consultées, le Cnis, la CNIL ainsi que le Comité de protection des personnes pour les recherches en biologie (CPPRB) s'il y a des prélèvements biologiques ».

Néanmoins, en privé et parfois même en public, les chercheurs ne dissimulent pas leur réticence à devoir justifier de leurs projets auprès des juristes de la CNIL. S'ils admettent volontiers qu'il y a des précautions à prendre, ils considèrent que ni les contenus de leurs fichiers ni l'usage qu'ils en font ne comportent des dangers pour les libertés individuelles. S'ils considèrent tout à fait opportun que la CNIL s'occupe des fichiers de la police, des banques ou des assurances, … ils trouvent un peu déplacé qu'elle s'occupe aussi de leurs fichiers.

Il reste que la loi existe et qu'il faut faire avec. Mieux, il faut prévenir les attaques plus ou moins malveillantes que des associations, des syndicats ou des organisations politiques pourraient mener contre leurs projets au nom de la protection des libertés individuelles. D'où les affirmations un peu solennelles selon lesquelles la confidentialité est une exigence essentielle qui retient toute leur attention.

1.3- La mise en avant de solutions techniques

« …Les possibilités offertes par les nouvelles techniques d'anonymisation »… « Des techniques perfectionnées, agréées par la CNIL, existent désormais ».

Lorsque l'on présente à des chercheurs ce qu'est un système de sécurité fiable, du type de ceux que l'on trouve dans certains secteurs de l'énergie ou des communications, dans la R&D des grandes entreprises, évidemment dans l'armement, … ils rétorquent immédiatement que ceci est inapplicable à leur travail : c'est trop cher et, surtout, c'est trop contraignant dans le travail courant. Il faut donc trouver « *Des techniques perfectionnées, ... qui offriront toute satisfaction aux statisticiens et aux responsables de l'opération*[9] ».

En clair, ces techniques doivent être transparentes pour les chercheurs, ils doivent faire de la sécurité sans avoir à y penser. Et ceci non seulement pour le confort de leur travail mais aussi pour la sécurité elle-même : s'ils doivent y penser, leur direction est convaincue, à tort ou à raison, qu'ils n'y penseront pas et il n'y aura donc pas de sécurité.

De telles « solutions techniques » seraient (peut-être ?) idéales mais les concepteurs pressentent qu'il faut encore beaucoup de réflexion et de groupes de travail pour y parvenir[10].

1.4- Une contestation pratiquement impossible

La lecture du compte-rendu de séance, aussi épuré soit-il, fait état d'objections soulevées par les participants quant à la sécurité d'une telle base de données. Le représentant de la CGT, la responsable d'un grand laboratoire du CNRS, le président de la commission lui-même posent des questions à ce sujet.

Les réponses sont tout à fait rassurantes : nous nous occupons sérieusement de ces aspects et sommes en relation avec la CNIL.

Dès lors, que peut-on dire de plus ? Qui a les moyens de savoir comment la sécurité est assurée dans ces organismes ? Certains de ceux-ci - pas tous loin de là ! - disposent d'une politique de sécurité un peu suivie mais elle n'est évidemment pas accessible au public et la façon dont elle est appliquée est strictement confidentielle. Même si tel ou tel incident pouvait être évoqué, notamment parce qu'il a été cité dans les médias, la direction de l'organisme n'aurait aucun mal à expliquer que des mesures, voire des sanctions, ont été prises, que la faille a été corrigée dans les meilleurs délais et qu'il n'y a eu aucune conséquence dommageable pour les personnes fichées.

Il faut pourtant mettre en doute la sécurité qui existe dans ces organismes faisant de la recherche en sciences sociales. Sans entrer dans les détails, on observe que la majorité des chercheurs en sciences sociales sont inconscients des contraintes de sécurité posées par l'informatique actuelle[11]. Les moyens d'identification et d'authentification sont

---

[9] On est presque ici au niveau du lapsus…

[10] On peut d'ailleurs s'inquiéter qu'une demande de conseils sur un tel sujet soit adressée au CNIS alors qu'il n'a aucune compétence en la matière.

[11] Il y a 20 ou 30 ans, de tels fichiers existaient déjà mais ils étaient confinés sur des systèmes centraux auxquels les accès étaient parcimonieux et difficiles. Si l'on trouvait une bande magnétique abandonnée dans le métro, qui

insuffisants[12], ils échangent allègrement les codes et les mots de passe, les fichiers circulent entre les postes professionnels et les postes familiaux, par réseau, par clé USB ou gravure de CD… Les fichiers circulent entre collègues d'une même promotion ou d'un même groupe d'enseignement, etc. Lorsque des accès sont restreints, les listes d'habilitation sont mal gérées ou pas gérées du tout…

Il n'y a pas lieu d'ailleurs de s'en étonner outre mesure : la sécurité est quelque chose de difficile et de coûteux à mettre en place et à faire fonctionner correctement. Pour les entreprises, le caractère vital de certains fichiers (les clients, les factures, la comptabilité, le personnel…) les a obligées à les sécuriser. Dans les organismes de recherche, cette obligation ne porte que sur quelques informations de gestion (la paye, les primes, le personnel, le budget…) et elle est assurée le plus souvent par le service informatique lui-même. Pour les fichiers des chercheurs, c'est une autre affaire…

Mais finalement, qu'il y ait des doutes ou qu'il n'y en ait pas, le résultat est le même : en droit français, la bonne foi se présume et si les représentants autorisés de ces organismes disent que la sécurité est assurée, on est bien obligé de les croire. En conséquence, la commission du CNIS, consultée pour donner son avis, devant autant de science et de conscience ne peut que donner un avis favorable. Après quoi, le projet va suivre son cours et personne ne pourra aller voir de plus près quelle est la fiabilité de la sécurité en place.

2- Comment améliorer la situation ?

Cette situation n'est pas satisfaisante. Tout d'abord, bien entendu, pour les personnes fichées. Parfois sans qu'elles n'en sachent rien, c'est un ensemble d'informations qui existent sur elles et qui peuvent être accessibles à des personnes non autorisées. A tort ou à raison, les personnes interrogées sont sceptiques pour ce qui est de la confidentialité de leurs réponses. Ceci finit par avoir un effet négatif sur les taux de réponse et, finalement, sur la qualité des résultats.

Pour les organismes également, le scepticisme produit des effets négatifs, dans la mesure où il est difficile d'enrayer ce mouvement de défiance. Pour les services ou les projets qui, souvent à contre courant, essayent d'améliorer leur sécurité, il est très difficile de ne pas être emporté dans le scepticisme général. A l'intérieur de l'organisme, il ne manque pas de bons apôtres pour soutenir, la main sur le cœur, que la sécurité est une exigence incontournable mais qu'il n'y a qu'une exigence de moyens et non de résultat. Dès lors, une sécurité « Canada Dry » est peut être suffisante

Pour sortir de cette situation, la proposition que je soumets ici à discussion consiste à faire intervenir un tiers qui expertisera la qualité de la sécurité des fichiers en cause et en rendra compte dans un rapport public. Elle s'inspire de situations analogues dans lesquelles

---

était capable de la lire ? Aujourd'hui, l'informatique des chercheurs est celle de tout le monde, mêmes machines, mêmes logiciels, mêmes réseaux, mêmes supports… Et si un CD-ROM contenant le fichier est trouvé dans le métro, il y aura de nombreuses personnes à pouvoir le lire.

[12] L'usage des certificats est rarissime pour contrôler l'accès aux données, y compris pour les postes nomades.

une partie est censée devoir faire confiance à une autre sans avoir la possibilité de vérifier a priori le fondement de cette confiance.

2.1- Utilité de l'intervention d'un tiers

Le premier exemple sera celui de la vérification de la comptabilité par le commissaire aux comptes. Dans son rapport à l'assemblée générale, l'entreprise explique à ses actionnaires que l'année a été difficile et qu'elle a préféré privilégier l'avenir -investir- plutôt que de verser des dividendes : les actionnaires doivent-ils faire confiance, quoiqu'il puisse leur en coûter ?

Pour sortir de ce type de situation, le droit commercial a prévu de faire intervenir un acteur extérieur à l'entreprise ayant pour rôle de contrôler la sincérité et la régularité des comptes établis par une société. Cet acteur, c'est le commissaire aux comptes. Membre d'une profession agréée, il va procéder à un audit comptable et financier sur lequel il va engager sa responsabilité[13]. L'entreprise sachant que sa comptabilité sera expertisée par le ou les commissaire(s) aux comptes est incitée à respecter strictement les normes. De l'autre côté, les actionnaires disposent du rapport d'audit pour fonder leur confiance. Dès lors les débats peuvent se dérouler sans arrières pensées ni procès d'intention.

Deuxième exemple : pour se différencier de ses concurrents et mettre en avant la qualité de ses prestations, l'entreprise va faire de la publicité et développer sa communication. En espérant que ses cibles voudront bien y croire. Elle peut aussi faire appel à un organisme extérieur accrédité – le certificateur – auquel elle demandera d'examiner tel ou tel processus de production en vue d'accorder ou non un label de qualité internationalement reconnu. C'est le principe des certifications ISO9000 qui apparaissent ainsi comme un outil de confiance entre clients et fournisseurs[14].

2.2- Application au domaine de la sécurité

Si on reprend l'exemple du Cnis sur le projet ELFE, voici comment les choses pourraient se passer.

2.2.1- Au niveau de l'avis d'opportunité

On se souvient qu'au terme de la présentation et du débat qui s'en était suivi, le président de la commission avait accordé un avis d'opportunité[15].

---

[13] L'article L.823-9 du code de commerce dispose que "Les commissaires aux comptes certifient, en justifiant de leurs appréciations, que les comptes annuels sont réguliers et sincères et donnent une image fidèle du résultat des opérations de l'exercice écoulé ainsi que de la situation financière et du patrimoine de la personne ou de l'entité à la fin de cet exercice."
Voir aussi : http://fr.wikipedia.org/wiki/Commissaires_aux_comptes

[14] Pour en savoir plus : http://fr.wikipedia.org/wiki/ISO9001
http://www.industrie.gouv.fr/portail/pratique/generalites.html

[15] : « Sous ces précautions, il n'y a pas d'objections ?
L'interformation [du CNIS] rend un avis d'opportunité favorable ».

Une autre réponse pourrait être la suivante :

« Compte-tenu des problèmes posés en matières de confidentialité par ce projet, la commission du Cnis demande que ses concepteurs soumettent à une prochaine réunion de la commission du Cnis les éléments ci-après.

A partir du cadre qui sera défini par la CNIL ou en accord avec elle, les concepteurs établiront le cahier des charges des mesures de sécurité à respecter.

Ce cahier des charges sera examiné par un cabinet d'audit en sécurité sélectionné sur appel d'offre, conjointement par les concepteurs du projet et le président de la commission du Cnis ou son représentant.

L'avis de la CNIL, le cahier des charges sécurité et le rapport du cabinet d'audit seront présentés à une prochaine séance de la commission du Cnis en vue de l'attribution d'un avis d'opportunité ».

Pour que le cabinet d'audit puisse réaliser son expertise, il a besoin de spécifications beaucoup plus précises que ce qui est inscrit dans le dossier de déclaration à la CNIL et/ou dans l'avis rendu par la CNIL. C'est pourquoi il est proposé de faire établir un cahier des charges des mesures de sécurité et ceci selon les normes établies. Cette tâche n'a rien d'extraordinaire. En effet, les questions de sécurité informatique, depuis le temps qu'elles se posent, ont été formalisées et normalisées[16]. En France, une commission de l'AFNOR a élaboré un référentiel des bonnes pratiques[17]. Intitulé « Sécurité des informations stratégiques, qualité de la confiance », il est sous-titré : « comment préserver la confidentialité des informations ». Il ne reste donc aux responsables du projet qu'à sélectionner les dispositions qui correspondent à leurs besoins. Pour le cabinet d'audit, le terrain de la sécurité est déjà bien balisé et l'expertise pourra être réalisée comme il en a l'habitude.

Pour la présentation au Cnis, il ne s'agit pas d'entrer dans le détail des mesures de sécurité[18] mais de recueillir le diagnostic du cabinet d'audit sur la conformité des mesures envisagées par rapport aux exigences de la loi, des normes en vigueur et des engagements pris.

2.2.2 – Pour la suite du projet

Si, notamment au vu du rapport « sécurité » du cabinet d'audit, la commission du Cnis a émis un avis d'opportunité favorable, il restera évidemment à vérifier que les mesures prévues auront et conserveront une réelle existence.

C'est pourquoi il serait bon d'envisager une périodicité à laquelle les concepteurs du projet devront faire expertiser la sécurité par un cabinet spécialisé, le rapport, étant là encore, présenté au Cnis. Pour la comptabilité de l'entreprise, les

[16] On se réfère ici à la norme ISO 17799. Voir par exemple http://www.computersecuritynow.com/
[17] Document AFNOR BP-Z 74-500 d'août 2002, 32 pages.
[18] Mesures qui n'ont d'ailleurs pas à être rendues publiques dès lors que cette publicité peut constituer une fragilité pour des personnes mal intentionnées.

commissaires aux comptes interviennent chaque année. Mais pour la certification ISO9000, le certificat est délivré pour plusieurs années. Dans le cas d'une application conçue pour durer plusieurs dizaines d'années, on pourrait concevoir des audits tous les ans ou tous les deux ans dans la phase de démarrage puis des audits plus espacés, tous les cinq ans, l'application étant en place. De tels examens réguliers sont souvent très utiles non seulement pour contenir les dérives que la routine peut introduire mais aussi pour mesurer l'impact des modifications diverses et fréquentes que subissent les systèmes d'information.

Conclusions

Certes une telle opération a un coût (à rapporter à l'ensemble du budget du projet) mais il semble que l'on peut en attendre un progrès considérable d'abord dans la protection de la confidentialité conformément à la loi de 1978 mais aussi dans la confiance que l'on peut accorder à ceux qui invoquent le caractère scientifique de leurs travaux pour nous demander des informations de plus en plus indiscrètes. Il ne s'agit pas forcément de limiter des possibilités de travail des chercheurs mais de subordonner la fourniture de telles informations à la mise en place de mesures de sécurité strictes, fiables et contrôlées de façon incontestable.

Cette intervention d'un tiers pour asseoir la confiance entre deux parties a été introduite ici dans le contexte des projets développés par des organismes de recherche en sciences sociales. Il conviendrait d'examiner comment ce type d'intervention pourrait s'appliquer dans d'autres contextes. Je pense notamment aux situations conflictuelles entre un organisme et son personnel à propos de la nature et de l'utilisation d'un fichier ou d'une base de données informatique. L'exemple que j'ai en tête est celui du fichier ANIS[19] à propos duquel ont surgi un certain nombre de conflits entre les organisations de travailleurs sociaux et les directions des conseils généraux à propos des données relatives aux bénéficiaires du RMI. Aux assistantes sociales exprimant des craintes sur la confidentialité des données, les directions répondaient qu'il n'y avait aucun problème. Dans ce type de situation où c'est la parole des uns contre la parole des autres, l'intervention d'un tiers qualifié ayant la confiance de chacune des parties pourrait faire avancer les choses : améliorer la sécurité et/ou la confiance.

[19] ANIS : une Approche Nouvelle de l'Information Sociale. Voir un exemple des problèmes posés par ce fichier : à l'adresse : http://www.delis.sgdg.org/menu/actionsociale/anis0698.htm