AVIS DE LA COMMISSION D'ACCÈS À L'INFORMATION

CONCERNANT LE PROJET DE

CONFIRMATION D'IDENTITÉ DE LA

CLIENTÈLE LORS DE LA PRESTATION

DE SERVICES DE LA

RÉGIE DES RENTES DU QUÉBEC

DOSSIER 01 11 09

SEPTEMBRE 2002

INTRODUCTION

1. LA PORTÉE DE LA DÉMARCHE

Le présent avis porte sur le processus de confirmation d'identité à distance d'un citoyen que la Régie entend déployer. L'appréciation en est une de pertinence et porte exclusivement sur l'analyse des documents déposés :

- Mémoire à la Commission d'accès à l'information, *L'identification électronique de la clientèle de la Régie des rentes du Québec lors de la prestation électronique de services*, 27 juin 2002, ainsi qu'un document complémentaire;

- renouvellement de la prestation des services à la Régie des rentes du Québec, présentation à la Commission d'accès à l'information, 19 juin 2002 (PowerPoint).

La sécurité de l'infrastructure soutenant la prestation électronique de services et l'intégrité des documents soutenant les transactions n'ont pas fait l'objet d'étude. Le projet de partenariat de services de la Régie et les services d'assistance aux clients n'ont pas non plus été évalués.

N'ont pas été analysées les communications de renseignements personnels et la qualité du consentement requis pour alimenter l'outil de simulation de retraite. Cet outil de simulation étant peu documenté, nous n'avons pu apprécier la circulation de renseignements personnels et les mesures assurant leur confidentialité. Nous ne nous prononcerons pas sur cette transaction. L'appréciation de la suffisance du type de confirmation d'identité proposé a donc été évaluée pour les services en ligne suivants : changement d'adresse, adhésion ou modification du dépôt direct et demande de rente de retraite.

2. LA DESCRIPTION DU PROJET

2.1 LE CADRE LÉGAL

Le recours à des moyens d'échanges électroniques dans la prestation de services est consacré dans le cadre légal québécois depuis l'introduction de la *Loi concernant le cadre juridique des technologies de l'information.*

Le *Code civil* reconnaît aux articles 2837 à 2839 l'équivalence des supports et la reconnaissance en preuve d'un document électronique comme un écrit.

> ***2837.*** *L'écrit est un moyen de preuve quel que soit le support du document, à moins que la loi n'exige l'emploi d'un support ou d'une technologie spécifique.*

Lorsque le support de l'écrit fait appel aux technologies de l'information, l'écrit est qualifié de document technologique au sens de la Loi concernant le cadre juridique des technologiques de l'information.

2838. *Outre les autres exigences de la loi, il est nécessaire, pour que la copie d'une loi, l'acte authentique, l'acte semi-authentique ou l'acte sous seing privé établi sur un support faisant appel aux technologies de l'information fasse preuve au même titre qu'un document de même nature établi sur support papier, que son intégrité soit assurée.*

2839. *L'intégrité d'un document est assurée, lorsqu'il est possible de vérifier que l'information n'en est pas altérée et qu'elle est maintenue dans son intégralité, et que le support qui porte cette information lui procure la stabilité et la pérennité voulue.*

Lorsque le support ou la technologie utilisé ne permet ni d'affirmer ni de dénier que l'intégrité du document est assurée, celui-ci peut, selon les circonstances, être reçu à titre de témoignage ou d'élément matériel de preuve et servir de commencement de preuve.

L'article 25.2 de la *Loi sur le régime de rentes du Québec* introduit la possibilité de recevoir un document électronique pour la Régie.

25.2. *La Régie peut, aux conditions qu'elle détermine, autoriser une personne qui doit lui transmettre un avis, un rapport, une déclaration ou quelque autre document à le lui communiquer au moyen d'un support magnétique ou d'une liaison électronique.*

En matière d'accès aux renseignements personnels par la personne concernée, les modifications apportées à l'article 84 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., chap. A-2.1, ci-après appelée Loi sur l'accès) permet l'accès à distance à ces renseignements par des technologies.

84. *L'organisme public donne communication d'un renseignement nominatif à la personne qui a le droit de le recevoir en lui permettant de prendre connaissance du renseignement sur place pendant les heures habituelles de travail ou à distance et d'en obtenir une copie.*

À la demande du requérant, un renseignement nominatif informatisé doit être communiqué sous la forme d'une transcription écrite et intelligible.

2.2 LES PRÉOCCUPATIONS DE LA RÉGIE

En matière de transaction électronique, la Régie reconnaît qu'elle « *doit pouvoir identifier une partie à un échange, avec des niveaux acceptables de certitude selon la nature de l'information à recevoir par la Régie ou celle des documents à émettre par celle-ci. La solution retenue doit permettre de démontrer le lien entre une personne et l'action qu'elle a posée pour la mise en preuve éventuelle.*

Ensuite, il importe de veiller à la conservation des documents; la Régie doit disposer d'un document fiable et utilisable en preuve, en cas de besoin. Il faut ainsi s'assurer de pouvoir établir la provenance d'un document, en identifier l'auteur, en protéger l'intégrité, en connaître la date de réalisation et, le cas échéant, de sa transmission à la Régie ou de son envoi par cette dernière.

De plus, une attention particulière doit être portée à la protection des renseignements personnels transmis à la Régie ou détenus par celle-ci. La solution doit en effet permettre la communication, dans un environnement sécurisé, des renseignements à la Régie. Cette solution doit également fournir les outils de sécurité nécessaires pour que seules les personnes autorisées aient accès aux données qui concernent une personne et qui sont détenues par la Régie.

Une quatrième préoccupation porte sur la possibilité pour la Régie de faire un envoi de manière sécurisée de l'information dont la communication est permise. La solution doit alors être en mesure d'assurer la protection de cette communication et de conserver des traces claires de celle-ci. ».

2.3 LES SERVICES EN LIGNE

La Régie entend rendre accessibles en ligne les services existants les plus utilisés et en introduire de nouveaux comme la fonction intégrée de simulation des revenus à la retraite. Les services en ligne sont destinés uniquement aux clients connus de la Régie.

« *Ces services en ligne seront beaucoup plus que de simples formulaires électroniques. Ils seront développés sous forme d'entretien électronique assisté et s'adapteront à la situation du client. L'accès, par le client, aux renseignements qui le concernent dans les banques de données corporatives de la Régie le dispensera de saisir des renseignements déjà connus et permettra de lui fournir, dans la majorité des cas, une réponse immédiate. La rapidité du traitement en ligne permettra aussi la validation instantanée des demandes du client et de lui signaler immédiatement si des erreurs ont été commises, évitant ainsi la multiplication des démarches par le citoyen, comme cela peut se produire avec les moyens traditionnels.* »

Les quatre services en ligne que la Régie entend déployer dans un premier temps sont les suivants :

- **le changement d'adresse** permet au client de voir s'afficher l'adresse actuelle détenue par la Régie et de pouvoir inscrire sa nouvelle adresse, ses numéros de téléphone de même que la date de prise d'effet de cette nouvelle adresse. La Régie confirme en ligne le changement d'adresse ou informe le citoyen d'une situation particulière qui exige un traitement administratif préalable;

- **l'adhésion ou la modification du dépôt direct** permet aux bénéficiaires d'inscrire ou de modifier les coordonnées bancaires requises pour le dépôt direct de leurs prestations. Lorsque l'institution bancaire est étrangère, le service en ligne n'est pas disponible puisqu'il requiert une signature;

- **la demande de rente de retraite** permet à un cotisant de soumettre sa demande et de connaître l'admissibilité et le montant de la prestation à recevoir;

- **la simulation des revenus à la retraite** vise à mettre en ligne un outil électronique de simulation des revenus à la retraite dans le but de sensibiliser le travailleur à l'importance de la préparation financière et de l'aider à atteindre une autonomie financière à la retraite. La simulation porte sur une projection de ses revenus bruts à la retraite exprimés en dollars d'aujourd'hui. La première étape permet d'identifier ses objectifs financiers en plus de fixer les paramètres de base utilisés pour estimer puis projeter les revenus à la retraite. La seconde étape permet d'estimer les revenus à la retraite en tenant compte des revenus générés par le Régime de rentes du Québec, les régimes de retraite et d'assurances (CARRA), le programme fédéral de la Sécurité de la vieillesse, les régimes complémentaires de retraite et l'épargne personnelle. La troisième étape projette le manque à gagner pour atteindre les objectifs exprimés par le cotisant par de l'information et des conseils.

2.4 L'ÉVALUATION DES RISQUES

La Régie a réalisé une évaluation des risques associés à la mise en ligne sur Internet des premiers services personnalisés. Les résultats de cette évaluation l'ont guidée dans la détermination du niveau de sécurité requis en matière de confirmation d'identité. Le niveau de risques global est fondé sur les menaces, la probabilité que ces menaces se concrétisent et sur les impacts anticipés sur la Régie et sur sa clientèle. « *Ainsi, les facteurs de risques retenus pour l'évaluation sont les suivants :*

- *la transmission de données en ligne du client vers la Régie (interception de données confidentielles);*
- *la transmission de données en ligne de la Régie vers le client (usurpation d'identité ou erreur d'identification – bris de confidentialité);*
- *la modification de données dans les banques corporatives de la Régie (intégrité);*

- *l'émission d'un paiement par la Régie (monétaire);*
- *la fréquence des transactions (impacts).* »[1]

L'analyse des risques fait ressortir que le vol d'identité peut avoir des impacts de perte monétaire, de bris de confidentialité à l'égard des renseignements personnels ou fiscaux de ses clients et de perte de réputation de la Régie. Cette même analyse fait aussi ressortir que le niveau de risques de concrétisation de la menace se définit comme « élevé » pour deux des services ciblés pour la mise en ligne court terme, soit le service « Outil de simulation de revenus à la retraite » et le service « Changement d'adresse ».

En considérant le niveau de risques « élevé », la Régie aurait pu exiger un processus d'authentification forte, comme une infrastructure à clé publique (ICP). Or, à court terme, ce processus ou un processus équivalent n'est pas disponible. La Régie a donc opté pour un processus qui consiste à mettre en place une identification de base mais qui est enrichie de critères spécifiques au type de clientèle, soit les cotisants et les bénéficiaires.

2.5 LES PRINCIPES DE LA CONFIRMATION D'IDENTITÉ

La Régie expose dans son mémoire les principes qu'elle entend observer :

« *La prestation électronique de services vise d'abord à faciliter l'accès, par les citoyens, aux services gouvernementaux et aux renseignements que l'État détient sur eux. […]*

Au-delà des moyens technologiques de sécurité, le processus d'identification constitue un élément essentiel pour assurer la confidentialité de l'information personnelle. Le processus d'identification doit, d'une part, être complet et robuste pour limiter les erreurs d'identification et l'usurpation d'identité et, d'autre part, être assez simple pour ne pas freiner l'accès aux services.

[…]

Le processus d'identification comprend deux étapes distinctes :

- *la première étape fait référence au processus par lequel le client fournit certains renseignements pour permettre à la Régie de la retracer dans ses banques de données;*
- *la seconde étape fait référence au processus par lequel la Régie vérifie que l'identité déclinée par le client est authentique et sienne. Cette vérification se fait par croisement de renseignements personnels utilisés comme éléments de corroboration.*

La Régie aura son propre processus d'identification qui consistera à identifier le client via le site de la Régie par l'utilisation de renseignements personnels comme éléments de corroboration.

---

[1] Régie des rentes, Mémoire à la Commission d'accès à l'information, Document complémentaire, *L'identification électronique de la clientèle de la Régie des rentes du Québec lors de la prestation électronique de services*, 27 juin 2002.

L'identification du client par la Régie s'effectuera donc à distance via le site de la Régie par un croisement de renseignements personnels entre ceux inscrits par le client et ceux contenus dans les banques de données de la Régie. »

La solution de confirmation d'identité exige que le client fournisse au moins deux renseignements personnels qui apparaissent sur des documents différents et acheminés à des moments différents chez lui par la poste. Pour répondre aux résultats de l'analyse de risques, le processus d'identification a été conçu afin de recueillir des renseignements personnels plus facilement accessibles par la personne concernée auquel on a ajouté des renseignements traités habituellement de manière secrète par le client et provenant de différentes sources. L'identification s'effectue en deux étapes.

D'abord, l'identification de base permet au client d'inscrire :

- **un numéro de référence** : numéro unique, non significatif, crypté et spécifique à l'accès électronique aux services émis par la Régie; il aura une durée de vie limitée et sera ajouté sur différents documents transmis par la poste aux clients de la Régie;
- **le numéro d'assurance sociale (NAS), la date de naissance et le nom de la mère**.

Ces renseignements sont comparés au contenu des banques de la Régie afin de retracer le dossier et de confirmer le statut du client (bénéficiaire ou cotisant).

Si les renseignements fournis correspondent aux renseignements détenus dans les dossiers de la Régie, le panorama d'identification enrichie lui permettra de fournir un renseignement personnel plus secret en fonction de son profil :

- si le client bénéficiaire reçoit ses prestations par dépôt direct, il s'agira du **numéro de compte bancaire**;
- si le client bénéficiaire reçoit ses prestations par chèque, il s'agira du **montant du dernier chèque**;
- si le client est cotisant, il fournira **le montant du revenu** déclaré selon sa plus récente déclaration de revenus (TP 1).

Ce n'est qu'après avoir franchi ces deux étapes que les services transactionnels deviendront accessibles. Le client devra suivre le processus complet d'identification à chaque visite, mais une seule fois par visite.

2.6 LES CONTRÔLES ET LA SÉCURITÉ

La Régie décrit dans son mémoire la façon dont elle entend exercer les contrôles :

« *Les transactions effectuées par le client à la suite de son identification seront journalisées de sorte qu'un lien puisse être établi entre ce client et les actes posés dans son dossier.*

[…]

L'accès au numéro de référence par le personnel de la Régie sera limité aux administrateurs du système et seulement lorsque requis. Les accès à ces numéros seront journalisés.

Le système de la Régie contrôlera les tentatives infructueuses d'identification. Après un certain nombre de tentatives d'identification, le numéro de référence utilisé sera désactivé. Lorsqu'un numéro de référence sera désactivé, le client devra demander un nouveau numéro. Au besoin, ce dernier pourra également communiquer avec la Régie pour valider les renseignements personnels d'identification.

En cas de perte du numéro de référence par le client, il sera possible de désactiver le numéro. »

Lors de la vérification d'identité, si plusieurs numéros de référence sont utilisés pour un même NAS, le numéro de référence correspondant à ce NAS est désactivé empêchant toute identification avec ce NAS.

« *La Régie met en place une infrastructure de sécurité adaptée à la prestation électronique de services. Elle offrira toutes les mesures requises et reconnues sur le marché : chiffrement des transactions, bastions, séparation d'environnements, détection d'intrusion, détection d'attaques de serveurs, gestion des accès contrôle des virus, contrôle des vulnérabilités, copie de sauvegarde, environnement redondant, politique de sécurité, architecture à plusieurs niveaux, relève, etc.* »

3. L'APPRÉCIATION

3.1 L'IDENTIFICATION À DISTANCE

L'entrée en vigueur de la *Loi concernant les technologies de l'information* de même que les modifications apportées à la Loi sur l'accès consacrent la possibilité de fournir un service à distance sans toutefois réduire les exigences en matière d'identification et de signature.

La Régie propose d'utiliser son site Web pour offrir ses services électroniques personnalisés.

Les technologies Web et l'Internet sont certes une voie privilégiée pour faciliter la communication entre la Régie et sa clientèle. Aussi, la Commission croit acceptable que la Régie transige avec sa clientèle via son site et qu'elle confirme l'identité à distance pour y offrir un service personnalisé.

Bien que le présent avis porte essentiellement sur l'opportunité de mettre en œuvre le processus d'identification soumis pour étude, la Commission souhaite mettre en garde la

Régie sur les vulnérabilités particulières amenées par l'utilisation des outils Web et de l'Internet. Ce mode de communication a ceci de distinctif, l'organisme qui offre le service ne peut, à lui seul, garantir la sécurité et la confidentialité de la transaction.

En effet, ces technologies présentent de façon inhérente des failles sur le plan de la sécurité et les risques se doivent obligatoirement d'être partagés entre la Régie et son client. La Régie peut sécuriser de façon robuste son infrastructure, l'utilisation d'un réseau public, comme l'Internet et d'un fureteur Web, exige que le client soit invité à prendre des précautions pour assurer la sécurité et la confidentialité de la transaction. Plusieurs exemples illustrent les précautions à prendre :

- le client doit pouvoir effacer la mémoire cache à la fin de chaque session puisque certains renseignements personnels reçus ou transmis durant la session se trouvent sur le poste qu'il utilise;
- il doit s'assurer de fermer la session personnalisée adéquatement;
- il doit s'assurer que le sceau de sécurité est présent lors de la transmission de renseignements personnels;
- il ne doit pas utiliser le courrier électronique pour communiquer des renseignements personnels à moins de chiffrer l'information;
- l'utilisation d'un pare-feu personnel est souvent recommandée par les institutions financières offrant des services en ligne; etc.

À cet égard, la Commission demande à la Régie d'apporter une attention particulière au développement de fonctions simples et ergonomiques sur son site pour que sa clientèle, généralement inexpérimentée sur le Web, puisse aisément mettre en œuvre les mesures qui lui incombent.

Ce constat devrait amener la Régie à fixer et à faire accepter des conditions d'utilisation qui encadreront la relation électronique entre celle-ci et son client. La Commission demande donc à la Régie de mettre en œuvre toutes les mesures de sécurité lui permettant d'assumer la plus grande part de responsabilité au regard d'une transaction impliquant des renseignements personnels. La Commission lui demande ensuite de fixer les modalités de la convention à intervenir entre les parties. Il est impératif que le client soit informé des risques encourus, des mesures qu'il est responsable de mettre en œuvre et de la responsabilité résiduelle de la Régie au regard de la protection des renseignements personnels impliqués dans la transaction. Ces conditions d'utilisation devront être évolutives. Par exemple, de récentes failles avec les certificats SSL ont été signalées à la clientèle par certaines institutions financières utilisant ces certificats puisque ces institutions ne pouvaient colmater la brèche de sécurité. Ainsi, une alerte de sécurité informait les internautes de la situation et leur demandait d'appliquer les correctifs appropriés.

Il est usuel particulièrement dans les transactions commerciales de voir un tel partage des risques et les conséquences, le plus souvent financières, deviennent alors acceptables pour les parties. En matière de protection des renseignements personnels, l'organisme public porte seul la responsabilité des renseignements personnels qu'il recueille, détient, utilise et communique. De plus, on devra considérer que la réparation des conséquences potentielles

d’un bris de confidentialité est souvent plus complexe que le règlement d’un litige financier.

3.2 LA CONFIRMATION D’IDENTITÉ PAR UN CROISEMENT DE RENSEIGNEMENTS PERSONNELS

La confirmation d’identité à distance présente un défi aux nombreuses organisations publiques ou privées qui souhaitent offrir à leur clientèle des services personnalisés. Les traditionnelles cartes d’identité doivent être remplacées par des mécanismes permettant à l’organisation, qui a un devoir de confidentialité, d’obtenir des garanties raisonnables de l’identité de la personne et de prévoir la capacité de déposer en preuve les éléments l’ayant amenée à conclure à l’identité d’une personne.

L’identité à distance présente un risque plus élevé d’erreurs qu’une vérification d’identité en personne. Aussi, ce risque supplémentaire doit être considéré.

En matière de technologies nouvelles, il est opportun d’évaluer à la fois la sécurité et les garanties offertes par ces technologies, mais aussi les inconvénients inhérents à cette technologie, notamment les atteintes potentielles à la vie privée des utilisateurs. Ainsi, les certificats d’identité électroniques constituent des pièces d’identité pour les citoyens et leur permettent d’apposer une signature électronique. La Commission a émis des réserves sur l’utilisation d’un tel dispositif considérant les risques créés par les ICP au plan de la protection des renseignements personnels et a demandé que soit restreinte l’utilisation des ICP aux seules situations où une personne doit décliner son identité et apposer sa signature.

Dans un monde papier, la signature est souvent le moyen utilisé pour établir le lien entre un document et une personne. Dans un monde électronique, ce lien peut être établi de diverses façons, chacune offrant un niveau de garantie qui se doit d’être proportionnel et suffisant au type de transaction à intervenir.

« *C'est souvent en établissant un lien entre une personne et un document qu'il devient possible d'attribuer les droits et responsabilités relatifs à ce document.*

[…]

Le lien peut être assuré par tout procédé ou moyen permettant de les relier.

[…]

Pour atteindre ce résultat, on peut utiliser un procédé ou une combinaison de moyens de quelque nature que ce soit pourvu que les objectifs soient rencontrés. Les procédés peuvent être d'ordre technologique ou non. On ne privilégie pas la signature d'une personne comme moyen de faire le lien entre elle et un document et on ne l'y limite pas non

plus. L'article 39 de la loi la mentionne seulement comme étant l'une des possibilités pour établir un tel lien. »[2]

Aussi, la signature électronique permet d'atteindre une garantie irrévocable de l'identité de la personne et de l'acte juridique qu'elle pose. L'article 39 de la *Loi concernant le cadre juridique des technologies* précise :

> ***39.*** *Quel que soit le support du document, la signature d'une personne peut servir à l'établissement d'un lien entre elle et un document. La signature peut être apposée au document au moyen de tout procédé qui permet de satisfaire aux exigences de l'article 2827 du Code civil.*
>
> *La signature d'une personne apposée à un document technologique lui est opposable lorsqu'il s'agit d'un document dont l'intégrité est assurée et qu'au moment de la signature et depuis, le lien entre la signature et le document est maintenu.*

Les critères prévus au Code civil sont les suivants :

> ***2827.*** *La signature consiste dans l'apposition qu'une personne fait à un acte de son nom ou d'une marque qui lui est personnelle et qu'elle utilise de façon courante, pour manifester son consentement.*

« *L'usage d'une signature électronique est donc tout à fait possible si cette dernière constitue une marque personnelle utilisée couramment pour manifester son consentement.* »[3]

La confirmation d'identité par croisement de données parvient à fournir une certaine assurance que l'identité de la personne en ligne est bien celle qu'elle prétend être mais n'en fournit pas la certitude. De même, le modèle présenté par la Régie permet, selon la Commission, d'établir de façon adéquate le lien entre une personne et l'acte posé.

La nécessité d'apposer une signature ou non, au sens du Code civil, dans le cadre des services qu'entend déployer la Régie n'a pas été documentée, mais la Commission comprend que la Régie conclut que celle-ci n'est pas requise pour les services visés.

Aussi, la Commission est d'avis que la prestation électronique de services peut, lorsque la signature n'est pas requise, utiliser l'appariement de données afin de confirmer l'identité de la personne concernée. La confirmation d'identité par croisement de données est, dans

---

[2] *Loi concernant le cadre juridique des technologies de l'information* (L.Q. 2001, c. 32) - Texte annoté par l'équipe de recherche en droit du cyberespace du Centre de recherche en droit public (CRDP) de l'Université de Montréal, site Autoroute de l'information, Secrétariat du Conseil du trésor.

[3] Idem à la note 3.

ces circonstances, acceptable et même souhaitable compte tenu des risques associés aux mécanismes d'identification plus robustes.

3.3 QUALITÉ DE L'AUTHENTIFICATION

La Commission comprend que le modèle sous étude identifie le client à partir de deux types de renseignements personnels connus à la fois de la Régie et du client.

Un premier type de renseignements personnels est plutôt usuel. Il s'agit du NAS, de la date de naissance et du nom de la mère. La garantie de la confirmation d'identité tirée de ces renseignements est relativement faible compte tenu de la circulation de ces renseignements dans le quotidien d'un citoyen. Par exemple, le NAS d'un individu est détenu par son employeur, son institution bancaire, ses services de placements, Équifax, Hydro-Québec, plusieurs ministères dont la vocation est financière, l'école, la garderie, le camp de jour de son enfant, les organismes de charité à qui il a fait des dons… Autre exemple, le nom de la mère et la date de naissance se retrouvent à la Régie de l'assurance maladie du Québec, dans tous les établissements de santé fréquentés, dans le dossier scolaire…

Un second type de renseignements que nous qualifierons de plus exclusif est composé d'un renseignement financier (numéro de compte bancaire, montant du dernier chèque ou revenu déclaré) et d'un numéro de référence.

Le renseignement financier est un renseignement qui circule effectivement moins mais qui, selon la Commission, n'est pas secret. Par exemple, le numéro de compte bancaire est diffusé par un citoyen lorsqu'il fait des chèques ou lorsqu'il adhère au dépôt direct. Par ailleurs, ces renseignements sont relativement continus dans le temps, ce qui augmente leur circulation et les risques d'interception. Ainsi, par exemple, le montant d'un chèque de prestation d'allocation familiale est fixé pour un an et le revenu déclaré l'est une fois l'an.

Le numéro de référence est un renseignement exclusif entre le client et la Régie et vient apporter la force nécessaire à la confirmation d'identité. Ce numéro de référence étant stratégique, la Régie devra encadrer rigoureusement la gestion de ce renseignement ainsi que la procédure de diffusion et de renouvellement afin qu'il puisse conserver son caractère exclusif.

Considérant l'analyse qui précède, la Commission conclut que le modèle soumis par la Régie est suffisant pour offrir les services en ligne analysés et qu'elle permet d'attribuer un acte à une personne sans utiliser des mécanismes qui ajoutent des risques d'atteinte à la vie privée.

3.4 LA GESTION DU NUMÉRO DE RÉFÉRENCE

Compte tenu du rôle stratégique du numéro de référence, sa distribution et les conditions de renouvellement devront être strictement encadrées.

De plus, l'utilisateur de services en ligne devra être sensibilisé au caractère stratégique et personnel de ce numéro et être invité à ne pas le divulguer. La Régie devra convier un client qui a des raisons de croire que son numéro a circulé ou a été communiqué à un tiers de requérir un nouveau numéro de référence à la Régie afin d'éviter que ce tiers puisse transiger en son nom.

La Commission soumet à la réflexion de la Régie le fait que certains services bancaires électroniques reconnaissent leur client par un mot de passe que l'utilisateur doit remplacer par un mot de passe secret qui ne doit pas être dévoilé, ni être écrit. La Commission demande à la Régie d'évaluer la pertinence de permettre à un client de modifier son numéro de référence.

3.5 INTÉGRITÉ ET JOURNALISATION

La *Loi concernant le cadre juridique des technologies de l'information* précise qu'un lien doit exister entre un document et son auteur.

> ***38.*** *Le lien entre une personne et un document technologique, ou le lien entre un tel document et une association, une société ou l'État, peut être établi par tout procédé ou par une combinaison de moyens dans la mesure où ceux-ci permettent :*
> *1° de confirmer l'identité de la personne qui effectue la communication ou l'identification de l'association, de la société ou de l'État et, le cas échéant, de sa localisation, ainsi que la confirmation de leur lien avec le document;*
> *2° d'identifier le document et, au besoin, sa provenance et sa destination à un moment déterminé.*

La Régie précise que les transactions effectuées par le client à la suite de la confirmation de son identité seront journalisées de sorte qu'un lien puisse être établi entre ce client et les actes posés dans son dossier.

Afin de permettre aux journaux de représenter le lien entre une personne et une action et de préserver l'intégrité de ce lien, des mesures particulières devront être prises par la Régie afin de maintenir l'intégrité des journaux et des autres documents pouvant être admis en preuve.

3.6 MONITORING ET TRAÇAGE

Les documents soumis font référence à la mise en place de mécanismes permanents de lecture sur le comportement et la satisfaction du client.

La Commission comprend que le lien entre une identification et ses transactions sera maintenu grâce à la journalisation. Elle convient donc que l'utilisation de services transactionnels personnalisés fera l'objet de journalisation. La Commission souhaite toutefois rappeler que l'accès à des services anonymes ou purement informationnels (informations générales) durant une session personnalisée ne devra faire l'objet d'aucun traçage. Aussi, toute cueillette de renseignements personnels liée à l'utilisation des services électroniques devra répondre aux impératifs de nécessité de la Loi sur l'accès et l'internaute devra en être informé quelle qu'en soit la forme (témoins, webbugs…).

CONCLUSION

La Commission répond favorablement au projet de confirmation d'identité de la Régie dans le cadre de la prestation électronique de services. La Régie a développé une approche simple et efficace permettant aux internautes de transiger avec elle.

La Commission souligne la qualité de la présentation des documents soumis, notamment l'analyse d'impacts au regard de la protection des renseignements personnels et l'application des principes de la *Loi concernant le cadre juridique des technologies de l'information.*