République française

Ministère de la fonction publique et de la réforme de l'État

Le Ministre
N/REF/CAB/2001 -80/GB

Monsieur Pierre Truche
14 rue du Professeur Grinard
69007 Lyon

13 décembre 2001

Monsieur le Président,

Le Gouvernement a engagé le 15 novembre 2001 la deuxième étape du chantier de l'administration électronique. Ce chantier, avec d'autres, vise à faire de la France l'économie numérique la plus dynamique d'Europe.

Après la mise en ligne des documents administratifs et des textes publics (lois, débats parlementaires, décrets et arrêtés, rapports, etc.), et alors que se multiplient les téléservices interactifs, l'État se donne pour objectif que soient proposées en ligne, d'ici à 2005, toutes les démarches administratives des particuliers, des associations et des entreprises, ainsi que les paiements fiscaux et sociaux.

II s'agit de faire progressivement en sorte que chaque usager bénéficie des technologies de l'information et de la communication dans ses transactions avec les services publics et puisse notamment accéder rapidement à toutes les informations administratives, effectuer en ligne et de manière sûre toutes ses démarches avec les services publics, retrouver l'historique de ses démarches passées et stocker en ligne, à son gré et en toute sécurité, les données administratives qui le concernent.

Pour ce faire, un site personnalisé, mon.service-public.fr, sera proposé d'ici à 2005 à chaque usager pour lui permettre de gérer en ligne l'ensemble de ses relations avec l'administration.

La généralisation des téléservices publics implique de nouvelles formes de partage ou d'échange de données entre les administrations, et donc la définition de nouvelles règles. Les progrès attendus pour l'usager des nouvelles possibilités offertes, en particulier quant à l'ergonomie des systèmes mis en place, devront naturellement s'accompagner d'une forte sécurité des données personnelles nécessaire à la protection de la vie privée.

Cet équilibre doit être recherché de manière démocratique. C'est pourquoi un large débat public sur les modalités de mise en œuvre des téléservices publics et de mon.service-public.fr sera lancé, auquel la CNIL sera associée. I1 visera à définir de manière transparente, d'ici à la fin de l'année 2002, les fonctionnalités et les garanties offertes par l'ensemble du système.

Votre mission, pour laquelle vous êtes mandaté en compagnie de M. Jean-Paul Faugère, préfet de Vendée, et de M. Patrice Flichy, professeur de sociologie à l'université de Marne-la-Vallée, consiste à préparer ce débat.

Ainsi, vous remettrez d'ici le début de l'année 2002 un document de consultation ou « livre blanc », qui présentera les enjeux au regard des attentes des usagers ainsi que les options possibles pour mettre en œuvre mon.service-public.fr, Ce document sera rendu public. II sera le socle d'un débat public, qui se poursuivra tout au long du premier semestre 2002. Je souhaite, au-delà de ce « livre blanc », que vous preniez une part active à ce débat, sous la forme qui vous paraîtra la plus appropriée. La synthèse des débats publics sera ensuite rassemblée sous la forme d'un « livre vert » de propositions, que vous remettrez au gouvernement avant la fin du troisième trimestre 2002.

En particulier, vous examinerez l'intérêt et les difficultés de la mise en place d'une ou plusieurs carte(s) de signature électronique du citoyen, ainsi que les modalités possibles de distribution de ces cartes et les rapports que ces supports pourraient entretenir avec les titres d'identité.

Vous vous attacherez à travailler en concertation étroite avec la Commission nationale de l'informatique et des libertés (CNIL). Elle sera notamment invitée à toutes les auditions auxquelles vous procéderez et destinataire de l'ensemble des documents reçus ou produits dans le cadre de la mission. Le forum des droits sur internet sera également associé à vos travaux et pourra notamment accueillir les espaces interactifs de débat et de concertation que vous souhaiteriez mettre en œuvre.

Pour l'accomplissement de votre mission, vous bénéficierez du concours des services concernés de l'État, et notamment du Commissariat général du Plan, de la Délégation interministérielle pour la réforme de l'État (DIRE) et de l'Agence pour les technologies de l'information et de la communication dans l'administration (ATICA), ainsi que des services des ministères concernés et, tout particulièrement, de ceux du ministère de l'Intérieur.

Je vous prie d'agréer. Monsieur le Président, l'expression de ma considération distinguée.

Michel Sapin

République française

Ministère de la fonction publique et de la réforme de l'État

Le Ministre
N/REF/CAB/2001 -80/GB

Monsieur Jean-Paul Faugère
Préfet de la Vendée
Préfecture
29, rue de Lille
85922 La Roche-sur-Yon Cedex

13 décembre 2001

Monsieur le Préfet,

Le Gouvernement a engagé le 15 novembre 2001 la deuxième étape du chantier de l'administration électronique. Ce chantier, avec d'autres, vise à faire de la France l'économie numérique la plus dynamique d'Europe.

Après la mise en ligne des documents administratifs et des textes publics (lois, débats parlementaires, décrets et arrêtés, rapports, etc.), et alors que se multiplient les téléservices interactifs, l'État se donne pour objectif que soient proposées en ligne, d'ici à 2005, toutes les démarches administratives des particuliers, des associations et des entreprises, ainsi que les paiements fiscaux et sociaux.

Il s'agit de faire progressivement en sorte que chaque usager bénéficie des technologies de l'information et de la communication dans ses transactions avec les services publics et puisse notamment accéder rapidement à toutes les informations administratives, effectuer en ligne et de manière sûre toutes ses démarches avec les services publics, retrouver l'historique de ses démarches passées et stocker en ligne, à son gré et en toute sécurité, les données administratives qui le concernent.

Pour ce faire, un site personnalisé, mon.service-public.fr, sera proposé d'ici à 2005 à chaque usager pour lui permettre de gérer en ligne l'ensemble de ses relations avec l'administration.

La généralisation des téléservices publics implique de nouvelles formes de partage ou d'échange de données entre les administrations, et donc la définition de nouvelles règles. Les progrès attendus pour l'usager des nouvelles possibilités offertes, en particulier quant à l'ergonomie des systèmes mis en place, devront naturellement s'accompagner d'une forte sécurité des données personnelles nécessaire à la protection de la vie privée.

Cet équilibre doit être recherché de manière démocratique. C'est pourquoi un large débat public sur les modalités de mise en œuvre des téléservices publics et de mon.service.public.fr, sera lancé, auquel la CNIL sera associée. II visera à définir de manière transparente, d'ici à la fin de l'année 2002, les fonctionnalités et les garanties offertes par l'ensemble du système.

Votre mission, pour laquelle vous êtes mandaté en compagnie de M. Pierre Truche, magistrat, président honoraire de la Cour de cassation, président de la Commission de déontologie de la sécurité, et de M. Patrice Flichy, professeur de sociologie à l'université de Marne-la-Vallée, consiste à préparer ce débat.

Ainsi, vous remettrez d'ici le début de l'année 2002 un document de consultation ou « livre blanc », qui présentera les enjeux au regard des attentes des usagers ainsi que les options possibles pour mettre en œuvre mon.service-public.fr. Ce document sera rendu public. II sera le socle d'un débat public, qui se poursuivra tout au long du premier semestre 2002. Je souhaite, au-delà de ce « livre blanc », que vous preniez une part active à ce débat, sous la forme qui vous paraîtra la plus appropriée. La synthèse des débats publics sera ensuite rassemblée sous la forme d'un « livre vert » de propositions, que vous remettrez au gouvernement avant la fin du troisième trimestre 2002.

En particulier, vous examinerez l'intérêt et les difficultés de la mise en place d'une ou plusieurs carte(s) de signature électronique du citoyen, ainsi que les modalités possibles de distribution de ces cartes et les rapports que ces supports pourraient entretenir avec les titres d'identité.

Vous vous attacherez à travailler en concertation étroite avec la Commission nationale de l'informatique et des libertés (CNIL). Elle sera notamment invitée à toutes les auditions auxquelles vous procéderez et destinataire de l'ensemble des documents reçus ou produits dans le cadre de la mission. Le forum des droits sur internet sera également associé à vos travaux et pourra notamment accueillir les espaces interactifs de débat et de concertation que vous souhaiteriez mettre en œuvre.

Pour l'accomplissement de votre mission, vous bénéficierez du concours des services concernés de l'État, et notamment du Commissariat général du Plan, de la Délégation interministérielle pour la réforme de l'État (DIRE) et de l'Agence pour les technologies de l'information et de la communication dans l'administration (ATICA), ainsi que des services des ministères concernés et, tout particulièrement, de ceux du ministère de l'Intérieur.

Je vous prie d'agréer, Monsieur le Préfet, l'expression de ma considération distinguée.

Michel Sapin

République française

Ministère de la fonction publique et de la réforme de l'état

Le Ministre
N/REF/CAB/2001 -80/GB

Monsieur Patrice Flichy
Professeur
UPRES
Université de Marne-la-Vallée
77454 Marne-la-Vallée Cedex

13 décembre 2001

Monsieur.

Le Gouvernement a engagé le 15 novembre 2001 la deuxième étape du chantier de l'administration électronique. Ce chantier, avec d'autres, vise à faire de la France l'économie numérique la plus dynamique d'Europe.

Après la mise en ligne des documents administratifs et des textes publics (lois, débats parlementaires, décrets et arrêtés, rapports, etc.), et alors que se multiplient les téléservices interactifs, l'État se donne pour objectif que soient proposées en ligne, d'ici à 2005, toutes les démarches administratives des particuliers, des associations et des entreprises, ainsi que les paiements fiscaux et sociaux.

I1 s'agit de faire progressivement en sorte que chaque usager bénéficie des technologies de l'information et de la communication dans ses transactions avec les services publics et puisse notamment accéder rapidement à toutes les informations administratives, effectuer en ligne et de manière sûre toutes ses démarches avec les services publics, retrouver l'historique de ses démarches passées et stocker en ligne, à son gré et en toute sécurité, les données administratives qui le concernent.

Pour ce faire, un site personnalisé, mon.service-public.fr, sera proposé d'ici à 2005 à chaque usager pour lui permettre de gérer en ligne l'ensemble de ses relations avec l'administration.

La généralisation des téléservices publics implique de nouvelles formes de partage ou d'échange de données entre les administrations, et donc la définition de nouvelles règles. Les progrès attendus pour l'usager des nouvelles possibilités offertes, en particulier quant à l'ergonomie des systèmes mis en place, devront naturellement s'accompagner d'une forte sécurité des données personnelles nécessaire à la protection de la vie privée.

Cet équilibre doit être recherché de manière démocratique. C'est pourquoi un large débat public sur les modalités de mise en œuvre des téléservices publics et de mon.service-public.fr sera lancé, auquel la CNIL sera associée. II visera à définir de manière transparente, d'ici à la fin de l'année 2002, les fonctionnalités et les garanties offertes par l'ensemble du système.

Votre mission, pour laquelle vous êtes mandaté en compagnie de M. Pierre Truche, magistrat, président honoraire de la Cour de cassation, président de la Commission de déontologie et de la sécurité et de M. Jean-Paul Faugère, préfet de Vendée, consiste à préparer ce débat.

Ainsi, vous remettrez d'ici le début de l'année 2002 un document de consultation ou « livre blanc », qui présentera les enjeux au regard des attentes des usagers ainsi que les options possibles pour mettre en couvre mon.service-public.fr. Ce document sera rendu public. II sera le socle d'un débat public, qui se poursuivra tout au long du premier semestre 2002. Je souhaite, au-delà de ce « livre blanc », que vous preniez une part active à ce débat, sous la forme qui vous paraîtra la plus appropriée. La synthèse des débats publics sera ensuite rassemblée sous la forme d'un « livre vert » de propositions, que vous remettrez au gouvernement avant la fin du troisième trimestre 2002.

En particulier, vous examinerez l'intérêt et les difficultés de la mise en place d'une ou plusieurs carte(s) de signature électronique du citoyen, ainsi que les modalités possibles de distribution de ces cartes et les rapports que ces supports pourraient entretenir avec les titres d'identité.

Vous vous attacherez à travailler en concertation étroite avec la Commission nationale de l'informatique et des libertés (CNIL). Elle sera notamment invitée à toutes les auditions auxquelles vous procéderez et destinataire de l'ensemble des documents reçus ou produits dans le cadre de la mission. Le forum des droits sur internet sera également associé à vos travaux et pourra notamment accueillir les espaces interactifs de débat et de concertation que vous souhaiteriez mettre en œuvre.

Pour l'accomplissement de votre mission, vous bénéficierez du concours des services concernés de l'État, et notamment du Commissariat général du Plan, de la Délégation interministérielle pour la réforme de l'État (DIRE) et de l'Agence pour les technologies de l'information et de la communication dans l'administration (ATICA), ainsi que des services des ministères concernés et, tout particulièrement, de ceux du ministère de l'Intérieur.

Je vous prie d'agréer, Monsieur, l'expression de ma considération distinguée.

Michel Sapin

Sommaire

Lettre de mission

Introduction 13

Première partie
Toile de fond 17

Chapitre 1
Nouveaux enjeux, nouvelles approches de la protection de la vie privée 19
Les risques et les inquiétudes en matière de vie privée se sont déplacés des « grands fichiers » vers les « traces », des administrations vers les opérateurs privés 19
Complémentarité de la loi et de la technologie dans la protection de la vie privée 20
Encadrement par le haut, contrôle par le bas 22
De nouveaux principes se cherchent : consentement, disposition des données personnelles 27

Chapitre 2
Problématiques des identités numériques 31
Multiplication, complexification, numérisation des identités 31
Vers une gestion des identités numériques 34
Grandes manœuvres commerciales et industrielles autour de la gestion des identités numériques 35

Chapitre 3
L'État, garant de l'identité ? 39
Nouvelle procédure : le titre fondateur 40
Une carte d'identité électronique 41

Chapitre 4
Vers l'administration électronique 43

Quelle administration électronique ? 43

Administration électronique en France : où en sommes-nous ? 48

Où en sont nos partenaires internationaux ? 50

Chapitre 5
Quelle protection des données personnelles pour l'administration électronique ? 53

Le cadre juridique et la jurisprudence de la CNIL 53

Contrôle social ou amélioration service rendu au public ? 57

La loi et la CNIL ne font pas obstacle aux téléservices 58

Deuxième partie
Idées directrices 61

Les administrations et le public : un pacte de confiance à renégocier 63

Pluralité des accès 64

L'administration électronique n'a pas pour objectif, et ne saurait avoir pour résultat, de permettre à l'administration d'augmenter le niveau de contrôle et de surveillance des citoyens 65

Un grand nombre de téléservices s'effectuent et devront pouvoir s'effectuer de manière anonyme, sans contrôle d'accès ni identification 66

La maîtrise des données personnelles : un principe nécessaire mais à enrichir 66

Intérêt et limite des solutions dites de « coffre-fort électronique » 67

Quel que soit le degré d'implication et de délégation à des opérateurs tiers, l'État garde une fonction d'encadrement et de définition des règles 68

La sécurité des téléservices 71

Les choix français doivent être le plus harmonisés possible avec les choix européens 72

Troisième partie

Questions pour le débat 73

Chapitre 1
Statut des données personnelles 75

Les personnes sont-elles propriétaires des données qui les concernent ? **75**

Quelles limites au principe de maîtrise des données ? **77**

Faut-il bâtir l'administration électronique sur la base des systèmes d'information traditionnels, ou en déplaçant le centre de gravité des données personnelles vers l'usager ? **78**

Recentrage des systèmes d'information administratifs et individualisation **79**

Chapitre 2
Architecture de l'administration électronique 81

Code informatique, code juridique **81**

Un compte unique ou plusieurs « comptes thématiques » ? **82**

Quel type de « compte administratif personnalisé » ? **83**

Quelles modalités d'identification et d'accès à ce compte administratif ? **84**

Signature électronique et infrastructures à clefs publiques : une solution publique ou une panoplie de solutions ? **85**

Faut-il un support physique pour gérer les clefs et les signatures ? **86**

Une carte d'identité dotée d'une puce électronique pourrait-elle devenir l'outil d'accès aux téléservices publics ? **87**

Chapitre 3
Droits, services, fonctionnalités 89

Comment l'usager délègue-t-il aux administrations le droit d'utiliser ses données ? **89**

Peut-on rendre opérationnel le principe selon lequel tout accès ou modification des données personnelles qui concernent un usager dans les bases de données publiques devrait donner lieu à une notification ? **90**

Un « bilan des droits » régulier pourrait-il être organisé ? **90**

Secteur public, secteur privé : qui fournit les services d'administration électronique ? **91**

Chapitre 4
Pilotage et mise en œuvre 93
Mise en œuvre : comment déployer l'administration électronique ? 93
Comment favoriser l'utilisation des téléservices par les usagers ? 94

Conclusion 97

Contributions extérieures 99

Interconnexions, NIR et téléprocédures : position actuelle de la CNIL 101

Les enseignements d'autres administrations européennes et du secteur privé dans le domaine des services en ligne 107

Une approche des IGC et de leur organisation dans l'administration et les établissements publics 111

La problématique de la sécurité des systèmes d'information (SSI) 117

Les projets de téléservices du ministère de l'Intérieur 121

Le programme Copernic : identification des contribuables et protection des données personnelles 125

Net-entreprises 129

Les auteurs 131

Introduction

Le gouvernement a engagé, en novembre 2001, la généralisation des téléservices d'ici à 2005, ainsi que la création, à cette échéance, d'un point d'entrée personnalisé offrant à chaque usager un tableau de bord et une interface unique pour gérer l'ensemble de ses démarches en cours et à venir : ce projet a reçu le nom de « mon.service-public.fr ». Le gouvernement a souhaité que soit engagé parallèlement aux études techniques préparant ces évolutions un large débat public sur les moyens de préserver et de renforcer la protection des données personnelles dans le cadre de l'administration électronique, et notamment sur l'usage à cet effet de carte(s) électronique(s).

Ce débat public s'avère en effet indispensable.

• Indispensable, d'abord, au regard de l'objectif : une transformation radicale des relations des usagers avec administration, qui doit se faire dans le respect des principes républicains. L'administration électronique ne se veut pas seulement « au service » de l'usager ; elle se construit « autour » de lui. Elle se réorganise pour lui permettre d'entreprendre et de conclure l'ensemble de ses démarches sans se déplacer ni attendre.

Mais, dès lors que l'administration électronique apporte aux usagers des services tangibles, procure de réels avantages, la question de l'égalité d'accès se pose et se posera avec toujours plus d'acuité. Cette administration électronique sera-t-elle réservée aux seules personnes ou foyers équipés d'un ordinateur et connectés à internet ? Pourra-t-on accéder aux mêmes services à partir d'un téléphone ? à partir de bornes interactives dans les bâtiments administratifs ou de points d'accès publics ? à partir de n'importe quel guichet et avec l'aide d'un agent médiateur ?

• Ce débat public s'avère également indispensable au regard des efforts que suppose la généralisation des téléservices : effort budgétaire, investissements informatiques, réorganisations, création de processus communs aux différents systèmes d'information, interopérabilité entre systèmes. *« Passer de l'administration en silo à l'administration en réseau »*, ainsi que l'exprime Thierry Carcenac dans son rapport parlementaire *Pour une administration électronique citoyenne* : cet ambitieux chantier nécessite des

efforts constants et considérables. Il s'effectue, de surcroît, dans un contexte d'innovation technologique rapide et donc d'incertitude.

• Ce débat public s'avère indispensable, enfin et surtout, au regard des préoccupations relatives à la protection de la vie privée que suscite la mise en place d'une interface unique entre usagers et administrations, quelle que soit son appellation : portail ou guichet personnalisé, compte ou coffre-fort citoyen.

L'usager est aujourd'hui confronté à une administration cloisonnée, chaque administration posant les mêmes questions, demandant les mêmes pièces justificatives. L'« interface unique » devrait permettre à l'usager de communiquer certaines données à une administration, à charge pour celle-ci de les faire suivre à d'autres. Tout cela suppose que les administrations collaborent, et, le cas échéant, échangent des données entre elles.

Le déploiement des téléservices, la mise en place d'un compte administratif personnalisé vont donner lieu à des flux de données personnelles. Il faudra donc garantir, notamment pour les plus sensibles ou les plus confidentielles d'entre elles, que seule la personne (ou le foyer) peut y accéder et réaliser ses démarches. Il faudra aussi codifier, sécuriser les modes d'accès, repenser les systèmes d'identification et d'authentification. Il faudra arbitrer entre la facilité d'emploi, l'ergonomie des modes d'identification et leur niveau de sécurisation. La mise en place de l'administration électronique pourrait permettre en contrepartie à l'usager de reconquérir une certaine maîtrise de ses données personnelles. Il pourrait exercer en ligne, voire en temps réel, les droits d'accès et de rectification des données que l'administration détient sur lui. Un droit que la loi lui reconnaît depuis 1978, mais qui reste aujourd'hui assez largement théorique.

À quelles règles seront soumis les échanges de données entre services d'une même administration, entre administrations ? L'interopérabilité entre systèmes d'information entraîne-t-elle nécessairement une interconnexion généralisée des fichiers ? Il importe d'examiner de près ce que cette « deuxième étape de l'administration électronique » implique en termes de circulation et donc de protection des données personnelles.

Le temps dont nous disposons, pour cette réflexion et pour faire nos choix, est compté. La marche vers l'administration électronique s'observe en effet dans tous les pays de l'OCDE. Les priorités, les cheminements et les stratégies de mise en œuvre convergent assez largement entre pays. Et, sur de nombreux aspects, nos partenaires européens progressent très vite.

De surcroît, l'essor de l'administration électronique coïncide avec l'apparition d'offres techniques et commerciales qui se donnent explicitement pour objet d'aider les personnes à gérer leur(s) identité(s) numérique(s) et leurs données personnelles. Ces outils et ces services sont promus par des acteurs économiques qui opèrent, d'emblée, à l'échelle mondiale. Si l'État conserve le monopole, régalien, de l'attestation des identités, les sphères, connexes, de l'identification, de la gestion des identités numériques, de la signature électronique donnent lieu, d'ores et déjà, à d'âpres rivalités industrielles. C'est donc aujourd'hui que nous devons déterminer nos besoins, nos décisions, en matière de gestion de ces identités, avant que les systèmes opérationnels mis en place ne s'imposent à nous.

Un débat public est donc bien nécessaire. C'est l'objet de ce rapport que de fournir un ensemble de constats, d'analyses, de réflexions et de questionnements pour le préparer. Il s'attache, dans un premier temps, à dresser la toile de fond : les nouveaux enjeux et les nouvelles approches de la protection des données personnelles (chapitre 1), les problématiques qui se nouent autour des identités numériques (chapitre 2), les attentes vis-à-vis de l'identité publique et le rôle de l'État (chapitre 3). Après avoir esquissé à grands traits la mutation que recouvre la notion d'administration électronique, les réalisations françaises et étrangères (chapitre 4), le rapport examine le cadre juridique (loi de 1978 et doctrine de la CNIL) dans lequel l'administration électronique s'inscrit (chapitre 5).

La mission qui nous était confiée n'allait pas jusqu'à la formulation de recommandations. Il nous est apparu, cependant, utile de dégager dans une deuxième partie un socle de principes généraux qui pourraient guider la mise en œuvre de l'administration électronique.

Ce rapport formule enfin dans une troisième partie une série de questions, de nature assez différente : selon les thèmes, on pressent qu'il y a des équilibres à trouver entre des exigences contradictoires ; parfois, afin de clarifier les enjeux, nous avons esquissé des scénarios.

L'administration électronique désigne un vaste champ d'applications :
– les relations des usagers avec les administrations ;
– la contribution des administrations à l'animation du débat public : diffusion des données publiques essentielles, forums publics, consultations en ligne, et plus largement les nouveaux mécanismes de consultation des citoyens ;
– les relations des entreprises avec les administrations ;
– la mise en œuvre des techniques du commerce électronique aux marchés et achats publics (*e-procurement*) ;
– les nouveaux modes de travail et d'organisation au sein de l'administration : transformation des métiers, travail coopératif, télétravail.

La Mission s'est principalement intéressée au champ des relations des usagers – Français et étrangers – avec les administrations, là où se concentrent les principales préoccupations en matière de vie privée, de protection des données personnelles et de gestion des identités [1].

1. La Mission s'est intéressée aux téléservices destinés aux entreprises dans la mesure où certaines solutions mises en œuvre pour les entreprises peuvent un jour être proposées aux personnes. Il y a, par ailleurs, une zone de recouvrement entre personnes physiques et personnes morales : un très grand nombre d'entreprises sont unipersonnelles. Le volet proprement citoyen (au sens étroit du terme) de l'administration électronique (diffusion des données publiques, consultations publiques) ne relève pas d'une logique de « téléservice ». On peut cependant y rencontrer des problématiques de protection de la vie privée. Les consultations publiques, par exemple, soulèvent des questions d'identification et d'anonymat. La question du vote électronique n'a pas été abordée en tant que telle par la mission. En revanche, les questions liées à la carte d'électeur ou d'éventuelles téléprocédures d'inscription sur les listes électorales font pleinement partie de son champ de préoccupation.

La Mission a rencontré et auditionné une trentaine de personnes. Au cours d'une première journée d'audition, elle a procédé à un tour d'horizon des principales technologies de gestion des identités : opérationnelles, en cours de déploiement ou en projet. Au cours d'une seconde journée d'audition, elle a rencontré les acteurs et les porteurs des téléservices administratifs les plus avancés. Dans une troisième étape, elle a exploré un certain nombre de scénarios sur les formes que pourraient prendre les téléservices du futur, en s'efforçant de croiser les attentes des usagers (simplification, ergonomie), les exigences de protection de la vie privée, les contraintes et les promesses des technologies.

Contrairement à l'usage qui veut qu'une personne auditionnée expose son point de vue ou son projet, réponde aux questions, puis laisse la place à la suivante, les auditions se sont déroulées de manière largement ouverte. Les responsables des administrations, les experts et les professionnels se sont pliés de bonne grâce, sans ménager leur temps, à ce dispositif d'auditions croisées, chacun auditionnant les autres avant d'être entendu par eux. Ces points de vue croisés, ces libres échanges, ont considérablement nourri les réflexions de la Mission.

Elle a été accompagnée tout au long de ses travaux, et nourrie par les contributions de l'agence des technologies de l'information et de la communication dans l'administration (ATICA), de la délégation interministérielle pour la réforme de l'État (DIRE), de la commission pour les simplifications administratives (COSA), de La documentation française. Elle a également bénéficié des travaux de la Fondation internet nouvelle génération (FING). Enfin, la mission a conduit ses travaux en étroite relation avec la commission nationale informatique et libertés (CNIL), dont les services ont, notamment, assisté à l'ensemble des auditions.

Première partie

Toile de fond

Chapitre 1

Nouveaux enjeux, nouvelles approches de la protection de la vie privée

Les craintes en matière de protection de la vie privée se sont historiquement cristallisées face à l'État.

La première vague d'informatisation des administrations, dans les années 1960 et 1970, orientée principalement vers la quête de productivité (soucieuse aussi d'améliorer la connaissance et le contrôle des populations), manifestait assez peu de considération pour les questions de vie privée. Dès que les technologies furent disponibles, les administrations s'efforcèrent de constituer de grands fichiers, bâtis autour d'identifiant massifs (c'est-à-dire répertoriant de larges proportions de la population).

Les législations adoptées par la plupart des pays européens au cours des années 1970 et 1980 – à commencer, en France, par la loi « informatique et libertés » de 1978 – visaient, en premier lieu, à protéger les citoyens contre les tentations inquisitrices des administrations.

Les risques et les inquiétudes en matière de vie privée se sont déplacés des « grands fichiers » vers les « traces », des administrations vers les opérateurs privés

Les nouvelles formes de collecte et de traçage (internet, la biométrie), la dimension internationale de la collecte et des transferts de flux, la valeur marchande attribuée aux données personnelles, la puissance des moteurs de recherche permettant d'opérer des croisements, ont considérablement changé la nature des risques et leur perception.

La crainte principale ne réside plus dans les bases de données interconnectées, mais dans le croisement de flux d'informations de sources très diverses. Chaque individu est désormais fiché plusieurs centaines, voire plusieurs milliers de fois. *« Toute personne est en effet appréhendée*

par des traitements automatisés de données dans une très grande diversité de situations : comme écolier, étudiant, salarié, contribuable, candidat à un emploi, patient, assuré social, bénéficiaire de prestations sociales, électeur, abonné au téléphone, à l'électricité et au gaz, locataire, titulaire d'un compte en banque, voyageur sur une ligne aérienne, abonné à un journal, client d'une librairie ou d'un supermarché, personne nominativement sondée sur ses jugements ou ses habitudes de consommation... » [1]

Les préoccupations en matière de privée, corrélativement à multiplication des données qui circulent de façon beaucoup plus fluide, se déplacent aussi des administrations publiques vers les entreprises. La directive sur la protection des personnes à l'égard du traitement des données à caractère personnel [2] reflète cette nouvelle perception des risques. Elle rapproche le droit des fichiers publics et celui des fichiers privés. Elle continue cependant à organiser un contrôle spécifique des fichiers publics qui recèlent des enjeux particuliers de protection de données.

Complémentarité de la loi et de la technologie dans la protection de la vie privée

L'idée a surgi, très tôt, que la technologie pouvait constituer le meilleur rempart contre la curiosité de la police, des administrations et des acteurs économiques. C'est, naturellement aux États-Unis, en l'absence d'un cadre véritablement protecteur, que cette perspective d'une protection par la technique a pris corps : elle combine deux traits marquants de la civilisation américaine : foi dans la technologie et foi dans la responsabilité individuelle (*« chacun doit se protéger lui-même »*).

Sans doute convient-il de distinguer, dans cette quête de technologies protectrices de la vie privée celles dont l'emploi dépend directement de l'utilisateur (cryptographie), celles qui sont mises en œuvre par des prestataires spécialisés (comme les services d'anonymisation), et celles qui sont inscrites dans l'architecture des réseaux et des systèmes, comme le projet *Plateform for Privacy Preferences* (P3P) du W3C.

1. Guy Braibant, *Données personnelles et société de l'information*, rapport au Premier ministre, La Documentation française, 1999.
2. Directive n° 96/46/CE du Parlement européen et du Conseil du 24 octobre 1995.

Les technologies protectrices de la vie privée : panorama des outils [1]

Les technologies protectrices de la vie privée (PETs : Privacy Enhancing Technologies) constituent l'un des éléments des systèmes de protection de la vie privée avec la réglementation, l'autorégulation des acteurs économiques et le consumérisme/militantisme.

Dans la vision européenne et canadienne, les technologies protectrices de la vie privée sont perçues comme une méthode pour rendre effectif le droit à la vie privée. Parfois, aux États-Unis, les promoteurs des PETs prétendent éviter l'évolution réglementaire vers un niveau supérieur de protection juridique.

La cryptologie est souvent citée comme LA technologie protectrice de la vie privée. C'est une vision très incomplète. Sans prétendre à l'exhaustivité, les catégories suivantes peuvent être considérées comme des technologies ou services protecteurs de la vie privée :
– progiciels de chiffrement des méls et des documents joints ;
– stéganographie : technique qui consiste à dissimuler un message à l'intérieur d'un autre fichier ;
– génération de méls temporaires. Le texte des courriers n'est plus lisible passé un certain laps de temps ;
– génération de méls non rediffusables. Le destinataire du message ne peut pas le faire suivre à d'autres destinataires ;
– services d'anonymisation de la navigation. Pour visiter les sites web sans laisser de traces susceptibles de faciliter l'identification du visiteur ;
– Remailer *(re-achemineur), service qui permet d'envoyer des messages sans que le destinataire puisse identifier l'émetteur ;*
– services d'anonymisation des interventions sur les forums de discussion ;
– les gestionnaires d'identité virtuelle. Approche qui consiste à créer des personnalités virtuelles qui ne peuvent être rattachées à l'identité réelle de l'auteur. Ces personnes virtuelles peuvent alors consommer et communiquer sous un pseudonyme ;
*– cryptage des conversations en messagerie instantanée (*chat*) ;*
– Firewall *(logiciel pare-feu) personnel pour micro-ordinateur pour identifier la présence de* cookies *ou des* spywares*, voire pour en interdire l'accès ;*
– progiciels de suppression des « traces » présentes sur l'ordinateur, par exemple les cookies *ou le cache ;*

1. Source : *ePrivacy*, Arnaud Belleil, Dunod, 2001.

– *progiciel de cryptage d'informations figurant sur le PC, par exemple les « favoris » ;*
– *externalisation des données personnelles sur un disque dur distant ;*
– *progiciels* anti-spam*, pour filtrer les courriers électroniques non sollicités.*

Le standard P3P, promu par le W3C [1], permet aux internautes de reconnaître automatiquement en se connectant à un site la politique de protection des données du site. D'une protection « individuelle » ou « marchande » (confiée à des prestataires), on passe, avec le P3P, à une forme de protection collective.

L'idée selon laquelle les principes de protection de la vie privée doivent être incorporés dans l'architecture des systèmes techniques, dans le « code », pour reprendre l'expression du juriste américain Lawrence Lessig, suscite un intérêt croissant. Pour les juristes américains qui théorisent cette approche d'une incorporation du droit dans la technologie (la technologie rendant exécutoire la loi), il revient au débat public, et en dernière instance à l'autorité politique, de fixer des objectifs : il appartient ensuite aux ingénieurs et aux entreprises de traduire ces objectifs dans le fonctionnement des réseaux.

La tentation est forte d'opposer une conception américaine de la protection individuelle (se protéger soi-même) et la conception européenne de protection par le droit. Lors du débat, en Allemagne, sur la transposition de la directive européenne, l'école dite de la *« modernisation offensive »* (où se rangeaient les commissaires à la protection des données fédéraux et des Länder) souhaitait une réforme substantielle de la législation allemande, en vue *« d'améliorer la protection assurée actuellement dans leur législation »*. Cette même école revendiquait la *liberté de cryptographie*, au motif *« qu'il sera de plus en plus à la charge des citoyens de se protéger eux-mêmes en utilisant des logiciels de cryptographie »*.

Encadrement par le haut, contrôle par le bas

Pour sauvegarder la vie privée, la plupart des législations « informatique et libertés » ont consacré une double approche de la protection des données :
– un contrôle exercé, par le haut, par les autorités indépendantes : ce contrôle sur les fichiers et les traitements est exercé en amont (déclaration ou

1. *World Wide Web Consortium*, le principal organisme de standardisation de l'Internet.

demande d'autorisation selon le statut, public ou privé de l'organisme selon la nature des données et des traitements eux-mêmes) et en aval (contrôle *a posteriori*) ;
– un contrôle exercé, par le bas, par les personnes elles-mêmes : à travers les droits d'information et d'opposition, d'accès et de rectification et d'opposition, à travers les droits d'information, d'accès, de rectification et même d'opposition [1].

Droit à l'information préalable

Le contrôle par l'individu des données qui le concernent suppose de sa part la connaissance des fichiers dans lesquels il est recensé. Ce droit à l'information préalable conditionne l'exercice des autres droits tels que le droit d'accès ou d'opposition.

Il se manifeste par :
– une obligation d'information au moment de la collecte des données : lors du recueil de données nominatives, la personne doit être informée du caractère obligatoire ou facultatif des réponses, des conséquences d'un défaut de réponse, des destinataires des informations ainsi que de l'existence d'un droit d'accès. Les questionnaires doivent mentionner ces prescriptions (article 27 de la loi, décret n° 81-1142) ;
– la transparence des traitements automatisés ;
– les actes réglementaires portant création de traitements dans le secteur public doivent être publiés ;
– la CNIL tient à la disposition du public la liste des traitements qui lui ont été déclarés avec mention de leurs principales caractéristiques (article 22 de la loi).

Le non-respect de ce droit est sanctionné pénalement (décret 81-1142).

Le droit d'accès

Le droit d'accès donne à toute personne la possibilité de connaître l'existence ou non de données la concernant dans un fichier automatisé ou manuel et, si elle le désire, d'en obtenir communication. L'exercice de ce droit permet à l'individu de contrôler l'exactitude des données stockées sur son compte et, au besoin, de les faire rectifier ou effacer (articles 34

1. Michel Sapin distinguait de la même manière *modèle global* (la loi) et *modèle individuel* (le « coffre-fort ») : *« Nous nous satisfaisons aujourd'hui d'un modèle "global" de la protection des données personnelles : on interdit quelques rapprochements de données, d'une manière qui reste opaque pour le citoyen. Parce que le développement technique l'autorise, nous voulons le compléter par un modèle "individuel". Demain, chaque citoyen disposera d'un "coffre-fort" électronique accessible seulement par lui, et en toute confidentialité. Il y gérera l'ensemble de ses échanges avec les administrations. Il l'utilisera pour connaître en temps réel et, le cas échéant, autoriser au cas par cas, les accès effectués par les administrations aux données le concernant. »* (Michel Sapin, Hourtin, août 2001).

à 38 de la loi). Le droit d'accès s'exerce directement par l'individu auprès de l'organisme détenteur d'informations le concernant [1].

Certaines données nominatives ne sont pas directement accessibles par les personnes concernées mais sont néanmoins soumises à un contrôle indirect :
– les informations à caractère médical ne peuvent être communiquées au patient que par l'intermédiaire d'un médecin de son choix (article 40 de la loi) ;
– l'accès aux informations utilisées dans les traitements intéressant la sûreté de l'État, la défense et la sécurité publique est médiatisé par un commissaire de la CNIL, membre du Conseil d'État, de la Cour de cassation ou de la Cour des comptes [2].

La nouvelle loi (article 39 du projet adopté par l'Assemblée nationale) ne modifie pas fondamentalement le droit d'accès :
« Art. 39. – I. – Toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir :
« 1° La confirmation que des données la concernant font ou ne font pas l'objet de ce traitement ;
« 2° Des informations relatives aux finalités du traitement, aux catégories de données traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées ;
« 3° La communication, sous une forme accessible, des données qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ;
« 4° Les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé lorsque les résultats de celui-ci lui sont opposés. Toutefois, les informations communiquées à la personne concernée ne doivent pas porter atteinte au droit d'auteur au sens des dispositions du livre I^er^ et du titre IV du livre III du code de la propriété intellectuelle.
« Une copie des données est délivrée à l'intéressé à sa demande. Le responsable du traitement peut subordonner la déli-

1. La communication des données doit être fidèle au contenu des enregistrements et effectuée en langage clair. Une copie des enregistrements peut être obtenue à la demande moyennant l'acquittement d'une redevance (20 francs pour le secteur public et 30 francs pour le secteur privé) (arrêté du 23 septembre 1980).
2. Les membres de la CNIL chargés de ce droit d'accès indirect effectuent les investigations utiles, font procéder aux modifications nécessaires et notifient au requérant qu'il a été procédé aux vérifications (article 39 de la loi). Des décrets du 14 octobre 1991 prévoient, sous certaines conditions, la communication aux personnes qui s'adressent à la CNIL du contenu de leur fiche détenue par les Renseignements généraux et autorisent la Commission à indiquer aux requérants inconnus des « RG » qu'ils ne sont pas fichés.

vrance de cette copie au paiement d'une somme qui ne peut excéder le coût de la reproduction.
« En cas de risque de dissimulation ou de disparition des données, le juge compétent peut ordonner, y compris en référé, toutes mesures de nature à éviter cette dissimulation ou cette disparition. »

• Ouverture pour tous les traitements et non plus seulement ceux dont la liste est publiée en application de l'article 22, liste qui comprenait tous les traitements qui doivent être déclarés à la CNIL.

• Ouverture de la possibilité pour l'intéressé de demander à ce que soient « verrouillées » les données à caractère personnel le concernant (article 40 du projet).

Dans le cas des demandes de rectification ou d'effacement, la directive ajoutait une précision pour dispenser le responsable du traitement de la notification aux tiers de toute rectification, effacement ou verrouillage si cela s'avère impossible ou suppose un effort disproportionné, mais le projet de loi adopté par l'Assemblée nationale ne le reprend pas.

L'exercice en ligne du droit d'accès et de communication (car les deux sont complémentaires et sont posés en même temps par la loi) suppose sans doute au moins deux séries de conditions :
– une identification solide de l'intéressé, au moins pour l'accès à certaines des données. Vraisemblablement, c'est un cas où peut être exigé un certificat électronique renforcé ;
– dans l'organisation de l'administration, une remise à niveau colossale des systèmes d'informations. Il faudra évidemment des années avant que l'accès et la communication en ligne soient possibles dans la majeure partie des administrations.

Droit de rectification

Le droit de rectification constitue un complément du droit d'accès.

Toute personne peut faire corriger les erreurs qu'elle a pu déceler à l'occasion de la communication des informations la concernant. Ainsi, en cas d'inexactitude, elle peut exiger que ces informations soient rectifiées, complétées, clarifiées, mises à jour ou effacées (article 36 de la loi).

Indépendamment de toute demande, la loi met à la charge des détenteurs de fichiers une obligation de rectification d'office dès lors qu'une inexactitude est détectée (article 38 de la loi).

Le non-respect du droit de rectification est sanctionné pénalement (décret 81-1142).

Droit d'opposition

Toute personne peut décider elle-même de l'utilisation de données la concernant et a donc la possibilité de s'opposer à figurer dans certains fichiers ou de refuser la communication des informations qui la concernent à des tiers (article 26 de la loi).

Il existe différentes formes d'expression de ce droit d'opposition :
– le refus de répondre lors de la collecte non obligatoire de données ;
– la nécessité de donner son accord écrit pour le traitement de données sensibles telles que les opinions politiques ou les convictions religieuses (article 31 de la loi) ;
– la faculté de demander la radiation des données contenues dans les fichiers commerciaux ou de vente par correspondance ;
– la possibilité d'exiger la non-cession ou la non-commercialisation des informations.

Le droit d'opposition comporte deux limites :
– son exercice est subordonné à l'existence de raisons légitimes ;
– il n'existe pas pour de nombreux traitements du secteur public.

Le non-respect de l'opposition pour raisons légitimes d'une personne à un fichage est sanctionné pénalement (article 226-18 du code pénal).

Les « raisons légitimes » ont été peu précisées par la jurisprudence et restent donc une formule assez générale.

S'agissant plus particulièrement des traitements du secteur public, le sujet semble être resté relativement théorique. En particulier, la possibilité prévue par la loi que les actes réglementaires créant des traitements interdisent le droit d'opposition ne semble pas avoir été couramment utilisée. Il reste que divers actes réglementaires utilisent la possibilité prévue par la loi d'interdire le droit d'opposition, notamment les fichiers de sécurité (pour le fichier du système national d'information Schengen, voir l'article 7 du décret du 6 mai 1995).

Si on doit raisonner en théorie, on peut sans doute dire que ce droit d'opposition devrait être possible pour tous les traitements qui ne correspondent pas à des missions obligatoires de l'administration, c'est-à-dire qui ne lui sont imposées par aucun texte législatif ou réglementaire et qui ne correspondent pas à des services publics ou à des services publics obligatoires (exemple des écoles de musique municipales).

On peut en fait raisonner par analogie avec l'article 7 du projet adopté par l'Assemblée nationale, dont la logique est finalement très proche, puisqu'il instaure une obligation de consentement aux traitements de données qui est un symétrique du droit d'opposition, et qui précise donc les cas où un traitement peut être fait sans le consentement de l'intéressé :

« Art. 7. – Un traitement de données à caractère personnel doit soit avoir reçu le consentement de la personne concernée, soit être nécessaire à l'une des conditions suivantes :
« 1° Au respect d'une obligation légale incombant au responsable du traitement ;
« 2° A la sauvegarde de la vie de la personne concernée ;
« 3° A l'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;
« 4° A l'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ;
« 5° A la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée. »

Ces deux régimes de protection, « par le haut » et « par en bas », sont complémentaires et se renforcent mutuellement.

Force est de constater, cependant, que les droits d'accès et de rectification sont peu utilisés dans la pratique. *« Dans la pratique, les droits de l'usager sont restés assez formels, celui-ci n'ayant qu'une faible connaissance des fichiers détenant des données sur lui. Le contrôle des traitements est devenu surtout l'affaire de la CNIL ».* [1]

Information, accès, rectification, opposition. Ces droits, qui ne peuvent aujourd'hui s'exercer que par courrier, trouveront, dans l'avenir, à s'exercer de manière plus effective, dès lors qu'il sera possible de les exercer en ligne. C'est d'ores et déjà le cas, dans un grand nombre de situations, pour le droit d'opposition.

De nouveaux principes se cherchent : consentement, disposition des données personnelles

Du droit de s'opposer, on passe, progressivement, à un principe de consentement, c'est-à-dire à la nécessité de recueillir l'accord préalable d'une personne pour stocker, traiter ou communiquer des données personnelles la concernant. Ainsi, dans le domaine de la santé, comme pour les autres familles de « données sensibles », le principe de consentement revêt

1. Herbert Maisl, conseiller d'État, « De l'administration cloisonnée à l'administration en réseau : fin de la vie privée et/ou satisfaction de l'usager ? », colloque « L'administration électronique au service des citoyens », 21-22 janvier 2002.

une acuité particulière. La personne doit donner son consentement explicite pour que ses données de santé fassent l'objet d'un traitement [1].

L'Allemagne a donné à ce principe, une valeur constitutionnelle. En décembre 1983, la Cour constitutionnelle, dans un jugement relatif au recensement de la population, a proclamé *« le droit d'autodétermination informationnelle »*, qui est le droit, pour chaque individu, de décider de la communication et de l'emploi des informations relatives à sa personne.

La directive européenne sur la protection des données à caractère personnel consacre ce principe de consentement. Elle définit le *« consentement de la personne concernée comme toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement »*.

Ce principe est repris, sous une forme plus ferme et plus ramassée, dans l'article 8 de la Charte des droits fondamentaux de l'Union européenne :
« 1. Toute personne a droit à la protection des données à caractère personnel la concernant.
« 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du ***consentement*** *de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.*
« 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante ».

Le consentement peut s'exprimer de diverses manières. La mise au point finale de la directive du Parlement européen sur le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (qui porte sur la collecte des données individuelles en ligne, et notamment, celle des adresses électroniques) a ainsi donné lieu à une âpre confrontation entre partisans du régime de l´*opt-in* (consentement préalable) et partisans de l´*opt-out* (démarche volontaire pour se faire rayer d'une liste) [2]. En tout état de cause, la revente à des tiers des données personnelles n'est pas autorisée sans consentement préalable.

1. Son consentement est nécessaire pour qu'elles puissent être transmises. La mise en place de la carte Vitale a suscité, en France, un débat très vif sur les risques d'une circulation incontrôlée de l'information sur la santé des personnes, la nature des données qui pourraient ou non être enregistrées sur la carte Vitale 2, les conditions dans lesquelles le patient autorise des professionnels de santé à accéder à tout ou partie de son dossier. Avec le développement des projets de « dossier médical » en ligne, le débat sur la maîtrise du « carnet de santé » se déplace de la carte Vitale vers la maîtrise par le patient du dossier médical en ligne.
2. Un troisième terme se cherche avec le *« soft opt-in »* : les entreprises qui auront obtenu directement du client ses coordonnées, à l'occasion d'un achat en ligne, pourront s'en servir pour leur propre prospection commerciale, sauf si le consommateur s'y oppose expressément.

Dans un univers où les fichiers administratifs ne sont pas simplement un danger pour la vie privée mais avant tout un élément de la vie quotidienne de chacun permettant l'apparition de services privés et publics en ligne, de nouvelles attentes se préciseront. Puisque l'usage des réseaux se répand et que les services publics en ligne ne sont pas redoutés mais plutôt attendus avec impatience, il ne suffira plus de protéger l'individu vis-à-vis des traitements de données, mais il faudra aussi lui permettre de tirer parti de ces traitements de données.

Un nouveau droit qui garantirait, au-delà de l'accès et de la communication, la libre disposition des données, c'est-à-dire l'autodétermination par une personne de l'usage des données qui le concernent, pourrait ainsi s'esquisser.

Chapitre 2

Problématiques des identités numériques

Transmettre son identité (identification), la faire reconnaître (authentification), la faire suivre d'un opérateur à un autre... Autour de l'identité numérique se cristallise une série de questions, pour partie assez anciennes, pour partie largement inédites.

Multiplication, complexification, numérisation des identités

Le concept même d'**identité numérique** n'est pas, et pas plus que l'identité « traditionnelle », univoque et uniforme.

Compte tenu de la polysémie des notions (identité, identifiant, identification), il convient avant tout de distinguer les différentes facettes de l'identité numérique.

• Au premier rang des identités numériques viennent les **« identifiants »**, ces numéros que les institutions attribuent à leurs assujettis, usagers, clients, membres. Ces « identifiants de gestion » permettent aux organisations de regrouper, sans ambiguïté, toute une série d'informations sur une même personne. Certains identifiants sont stables (c'est le cas de la plupart des identifiants administratifs), d'autres provisoires (on peut changer de banque ou de compagnie de téléphone). Certains concernent des populations restreintes (les clients d'une PME) ; d'autres sont « massifs » (le numéro INSEE) et concernent de larges pans de la population.

La loi délimite l'usage qui est fait de ces identifiants (le respect des finalités). La CNIL y veille, comme elle veille à ce que ces identifiants ne soient pas « signifiants » (c'est-à-dire qu'il soit impossible, à la simple lecture d'un identifiant, d'apprendre quelque chose sur la personne concernée, par exemple un numéro tiré au hasard). Ce n'est pas le cas du NIR, le numéro INSEE, par exemple, qui révèle immédiatement des informations sur le sexe, le lieu et la date de naissance.

Les identifiants sont au cœur des préoccupations de protection de la vie privée. Ils n'épuisent cependant pas le sujet. Les techniques de *datamining* permettent, par exemple, de reconstituer très efficacement le profil d'une personne sans recourir à un identifiant unique, par rapprochement de traces diverses au sein d'un système d'information.

L'identification consiste, pour l'usager, à indiquer qui il est avant d'accéder à une information ou un service. L'opérateur peut limiter l'identification aux nom, prénom, adresse ou numéro de téléphone, mais ce sont des informations qu'il est relativement facile de reconstituer pour usurper une identité : c'est pourquoi on recourt fréquemment à des mots de passe, codes d'accès, numéros personnels, etc. Quand un opérateur souhaite réserver l'accès à une catégorie de personnes (membres, affiliés, abonnés), quand l'opération présente le caractère d'une transaction ou revêt un caractère confidentiel, on opte, en général pour une identification plus sûre, qui combine un identifiant (fourni par l'opérateur et qui peut être signifiant) et un mot de passe (fourni par l'opérateur et modifiable par l'utilisateur ou choisi par l'utilisateur).

Les identifiants qui servent à s'identifier sont souvent distincts des « identifiants » utilisés par les organisations pour gérer les personnes. Mais, dans de nombreux cas, ce sont les mêmes. L'assuré social, par exemple, appose son identifiant INSEE sur les feuilles de soin de la sécurité sociale et accède par ce même identifiant (et un mot de passe) aux informations disponibles sur AlloSécu relatives à ses remboursements.

Identifier le service

Il faut enfin noter que l'identification pour un téléservice ne se borne pas à l'identification de l'usager : ce dernier doit également acquérir la certitude que le serveur sur lequel il est en train de réaliser une démarche est bien celui qu'il est censé être, et non une copie réalisée pour récupérer, par exemple, des données personnelles le concernant. Le label « .gouv.fr » par lequel se terminent la plupart des adresses de sites web et de courrier électroniques de l'État est un premier élément de réponse, qui ne vaut cependant pas pour les collectivités territoriales ou pour les services rendus sur d'autres terminaux (téléphone, notamment).

Certains estiment donc nécessaire que les administrations se dotent d'une infrastructure fiable d'identification de ses serveurs web et autres automates d'interaction avec le public. Elle pourrait prendre la forme d'une infrastructure unique de gestion de clefs d'identification des serveurs, reposant sur une autorité de certification de ces clefs unique gérée par le Secrétariat général à la défense nationale (SGDN).

• L'adresse postale a longtemps été et reste, assez largement la principale **« coordonnée de référence »**, pour l'administration comme pour les opérateurs privés. L'envoi d'un courrier permet de s'assurer qu'on s'adresse à la bonne personne, moyennant une vérification en amont (le justificatif de domicile, souvent une facture d'EDF ou d'un opérateur téléphonique) et une vérification en aval (un contrôle d'identité du destinataire par un agent de la poste pour le courrier recommandé). L'adresse postale perd cependant sa primauté comme coordonnée de référence. Certains opérateurs de service ne demandent plus l'adresse postale, ni même le téléphone, mais se contentent de l'adresse électronique.

• Pendant des millénaires, la **signature** manuscrite a tenu lieu (et tient encore lieu) d'instrument de preuve et d'authentification. Avec la directive européenne et la loi du 13 mars 2000, la loi reconnaît désormais la valeur juridique des procédés de signature électronique qui remplissent la double fonction d'authentification du signataire et de manifestation de son consentement au contenu de l'acte.

• L'utilisation d'un **pseudonyme** concernait, autrefois, un nombre limité de personnes : artistes et auteurs, principalement. Avec le développement du courrier électronique, des forums et des chats sur internet, des jeux en réseau, un grand nombre d'internautes utilisent des pseudonymes, se construisent des **identités artificielles**, **virtuelles**, parfois multiples. La question de l'anonymat sur les réseaux est complexe. « *L'individu veut se promener et agir librement comme dans sa vie quotidienne réelle, les entreprises veulent l'identifier pour mieux le servir, les autorités répressives ont besoin de retrouver les coupables d'infractions et donc de les identifier. L'équation est facile à poser, moins facile à résoudre :*
– l'individu doit pouvoir rester anonyme sur le réseau pour aller et venir, faire des paiements, envoyer des lettres...
– cet anonymat peut se faire au moyen de la pseudonymisation.
Cet anonymat ne saurait cependant interdire de retrouver l'identité des personnes si nécessaire « (en cas d'infraction) [1]. L'anonymat qui protégerait l'auteur d'une infraction est très relatif ; en réalité, les traces laissées par les utilisateurs au cours de leur navigation permettent souvent de remonter à la source de l'infraction [2].

Au total, l'identité numérique se compose d'un **ensemble d'identifiants partiels**, finalisés, et des relations qu'entretiennent ces identifiants.

1. *Les réseaux numériques*, rapport du Conseil d'État, 1998.
2. Le Conseil d'état s'interrogeait, en 1998, à propos des pseudonymes, sur l'émergence d'une « identité virtuelle » : *« on ne peut être incriminé pour un vol de pseudonyme qui n'est qu'un vol d'informations non sanctionnable en tant que tel (sauf utilisation frauduleuse de ce pseudonyme).* (...) *Quid de la création d'une identité virtuelle entièrement fausse portant le nom d'une personne réelle, agissant, parlant, communiquant mais sans liaison avec la personne réelle ? Ne faut-il pas dès lors repenser la protection de façon générale, en réfléchissant à la question des droits de la personne virtuelle, différents peut-être de ceux de la personne réelle ? »*, *Les réseaux numériques*, rapport du Conseil d'État, 1998.

L'essor de l'administration électronique et du commerce électronique multiplie et complexifie ces identités partielles et ces relations.

• Du point de vue de la protection de la vie privée, il faut veiller à ce que ces identités numériques (qui constituent autant de facettes de la personne) restent étanches et confinées chacune dans sa « sphère ».

• Du point de vue des usages se pose la question de la gestion et de l'interopérabilité des identités numériques.

Vers une gestion des identités numériques

Avec l'intensification des interactions en ligne ou avec des automates (lecteur de carte bancaire), les personnes sont sommées, plusieurs fois par jour, de décliner mots de passe et codes d'accès.

Cette multiplication d'identités et d'identifiants soulève quatre types de problèmes :
– comment mémoriser les différentes identités et identifiants (ainsi que les « droits » ou les « préférences » associés) ?
– comment rendre interopérables entre elles les coordonnées associées aux différents appareils (micro-ordinateur et téléphone mobile, voire assistant personnel), à différents fournisseurs ou réseaux ?
– comment faire en sorte que l'on puisse effectuer ces opérations (et donc transporter ses identités avec soi) dans des contextes différents : au travail, à domicile, en déplacement ?
– comment maîtriser la circulation des données personnelles associées à l'une ou l'autre des identités ? Selon le contexte, selon la nature de l'institution, selon les risques pressentis ou les avantages attendus, une personne souhaitera ne transmettre, avec son identité, qu'un minimum d'informations personnelles (seulement le nom, mais pas l'adresse postale ; seulement l'adresse électronique mais pas le nom ; le nom mais pas la profession). À l'inverse, elle communiquera des informations plus approfondies, et plus confidentielles, pour être mieux servie ou pour faciliter la transaction. Le cas échéant, elle souhaitera dissimuler entièrement son identité.

En bref, plusieurs problématiques se nouent ainsi autour des identités numériques : confort d'utilisation, ergonomie des services, sécurité des échanges, protection de la vie privée, etc.

Grandes manœuvres commerciales et industrielles autour de la gestion des identités numériques

Pratiquement tous les aspects de l'identité numérique évoqués plus haut donnent lieu à des offres de services ou à l'existence d'un marché. Le cadre juridique exerce une influence prépondérante sur la dynamique et la taille de ces marchés [1]. On peut notamment citer :

– le marché des logiciels de « gestion des relations clients » (GRC) : après avoir amorcé la refonte de leurs systèmes d'information autour leurs « clients », les banques et les entreprises de service se dotent de tels systèmes pour suivre au plus près les pratiques de leurs clients, anticiper leurs demandes, formuler des offres de services profilées ou personnalisées ;

– autour de cette ressource que sont les « coordonnées de référence » s'est développé un marché très actif de la vente d'adresses, des bases de données marketing et de la géolocalisation ;

– depuis l'adoption de législations sur la signature électronique, le marché du certificat électronique connaît un développement rapide. Des « infrastructures de gestion de clefs » se mettent en place à grande échelle pour faciliter l'accès aux services financiers, les relations interentreprises et les démarches administratives [2]. On trouve sur ce *marché de la confiance* des acteurs issus du monde du logiciel (VeriSign, Entrust, Baltimore, etc.), des cabinets de conseil, des banques, les opérateurs de télécommunications (France Télécom avec Certplus), des logisticiens (La Poste avec Certinomis), des places de marché, les chambres de commerce (ChamberSign), les industriels de la carte à puce (Gemplus, Schlumberger, Solaic, etc.) et bien d'autres. Ce secteur a vu émerger un acteur de premier plan, VeriSign. Cette société américaine spécialisée dans la sécurisation des transactions en ligne a d'ailleurs absorbé au printemps 2000 Network Solutions (qui assure l'enregistrement des principaux noms de domaines de l'Internet), Illuminet, un opérateur de télécommunications et Signio, spécialiste du traitement des paiements.

1. Ainsi, en l'absence d'un cadre protecteur en matière de données personnelles, des entreprises proposent à qui le souhaite, aux États-Unis, leur médiation pour faire retirer ses coordonnées des grands fichiers du marketing direct.

2. Ces infrastructures de confiance offrent électroniquement la garantie d'être en relation avec la bonne personne (validation), que celle-ci soit toujours autorisée à utiliser ses prérogatives dans le processus d'échange (habilitation), que la communication se fasse en toute confidentialité (encryption), que le contenu et/ou le contentant de l'échange soit correctement et juridiquement horodaté, signé et archivé (notarisation).

Personnalisation, identification et authentification [1]

La personnalisation consiste à adapter le service rendu à chaque usager. Beaucoup de services personnalisés peuvent être fournis sans identification, sur la base d'un simple pseudonyme sans lien avec l'identité de l'usager.

• L'identification consiste, pour l'usager, à indiquer qui il est avant d'accéder à une information ou un service.

• L'authentification consiste, pour l'usager, à prouver son identité, ce qui lui permet éventuellement de signer des transactions ou des actes.

Il convient de bien distinguer identification et authentification.

*• **Identification***

Les banques fournissent depuis des années des services en ligne (consultation de comptes, mais aussi télépaiement, virements, ordres de bourse) dont l'accès est protégé par un simple couple identifiant (fourni par la banque) – mot de passe (généralement fourni par la banque et modifié par l'utilisateur).

Une convention bilatérale, qui est parfois elle-même électronique, régit les règles d'usage et les responsabilités des parties.

Un tel dispositif d'identification « conventionnelle » ne remplit pas les conditions nécessaires à l'authentification. Il permet pourtant d'assurer des services extrêmement riches, comme la consultation du compte et bon nombre d'opérations.

*• **Authentification***

L'authentification est le niveau qui permet de remplir les conditions de validité d'une signature électronique, donc de valider des actes ou encore de protéger l'accès à des données particulièrement sensibles.

Les conditions de mise en œuvre de la signature sont cependant lourdes, notamment au départ (attribution d'un certificat numérique) ; en revanche, il est économiquement plus facile d'imaginer un dispositif d'authentification et des certificats « interopérables », c'est-à-dire qui permettent de s'authentifier vis-à-vis de plusieurs interlocuteurs distincts. A contrario, cette mutualisation des certificats nécessite une confiance accrue vis-à-vis du fournisseur du certificat (autorité d'enregistrement).

Un très grand nombre de téléservices peuvent être fournis (parfois de manière légèrement dégradée) au travers d'un

1. Source : Daniel Kaplan, Fondation internet nouvelle génération.

simple pseudonyme : l'utilisateur fournit à un portail un ensemble de données personnelles, mais celles-ci ne permettent pas de connaître son identité.

Ces données sont conservées et permettent de bénéficier d'informations « profilées ». C'est pour les autres services, qui nécessitent une identification plus forte que les identifiants classiques, que des solutions de type coffre-fort électronique doivent être examinées.

La gestion des identifications suscite de nouvelles offres techniques et commerciales. Elle est au centre d'une controverse très vive depuis que Microsoft a annoncé son projet *Passport*.

Avec *Passport*, Microsoft propose en effet une procédure unifiée d'identification, valable *a priori* pour l'ensemble des transactions en ligne. Concrètement, l'identification effectuée sur le premier site affilié *Passport* permet d'accéder à tous les autres sites affiliés sans avoir à ressaisir ses paramètres d'identification. L'internaute choisit simplement, à chaque changement de site, de passer du mode anonyme au mode identifié. Techniquement, *Passport* se décompose en deux modules : celui qui assure l'authentification et celui qui permet la gestion de données personnelles. Dans une première version, les deux modules étaient gérés et hébergés par Microsoft. Dans la nouvelle architecture proposée par l'éditeur, le module d'authentification resterait placé sous le contrôle direct de Microsoft, tandis que la gestion des données personnelles serait assurée par des fournisseurs de services indépendants (qui devront néanmoins acquérir la technologie *Passport* et s'y affilier, à moins que des solutions compatibles au standard Kerberos puissent être raccordées).

Le lancement de *Passport* a suscité, en réaction, la création d'un consortium nommé *Liberty Alliance*, initié par Sun Microsystems. On y trouve des acteurs des télécommunications (comme Nokia, Sprint, Vodafone, NTT DoCoMo, France Télécom), des fabricants de cartes à puces (notamment Gemplus et Schlumberger) et d'autres grands acteurs comme Cisco, la Bank of America, Ebay, RealNetworks, Verisign ou encore RSA Security. L'objectif de cette alliance est de créer et de déployer une alternative à *Passport* : une solution ouverte pour l'identification sur les réseaux, sans base de données centrale ni dispositif centralisé d'authentification.

Parmi les technologies émergentes dans ce champ de la gestion des identités numériques, il convient enfin de mentionner le projet Enum, porté par plusieurs organismes internationaux de normalisation des télécommunications et de l'internet (IETF, UIT, etc.). Enum est un service de regroupement d'identifiants qui vise à rendre interopérables le réseau de télécommunication téléphonique et le réseau internet. Concrètement, avec un seul numéro (de téléphone), il deviendrait possible de joindre une personne par téléphone, par courrier électronique, sur son téléphone mobile, etc.

Chapitre 3

L'État, garant de l'identité ?

La délivrance des titres d'identité et le droit de contrôler l'identité sont des prérogatives centrales de l'État.

Alors que les identités numériques prolifèrent, et que se développent à une échelle accrue des formes d'identité privées, semant le trouble sur la notion même d'identité, on va peut-être redécouvrir la valeur de l'identité publique, originelle et originale, unique, stable et permanente, attestée et garantie par l'État. L'identité publique, en un sens, sert déjà de socle et de référent pour certaines identités numériques. La carte d'identité n'est-elle pas demandée, dans bien des magasins, à l'appui d'un chèque ?

À y regarder de plus près, l'identité publique est d'abord un processus qui relie des registres (l'état civil), une combinaison d'informations (reliées au patronyme), des éléments matériels détenus par l'administration (photographie numérisée, empreinte digitale, etc.) et des titres d'identité.

L'identité au sens des informations qui figurent sur le registre d'état civil est aujourd'hui constituée des éléments suivants : le nom, un ou plusieurs prénoms, la filiation avec les prénoms et nom du père ainsi que les prénoms et nom de jeune fille de la mère, la date et le lieu de naissance. La combinaison de ces éléments (patronymie et filiation) constitue un identifiant performant : elle élimine les risques d'homonymie. À la différence du NIR [1], c'est un identifiant sans « fichier centralisé » : si les fichiers d'état civil sont numérisés, ils ne sont pas connectés. Il n'existe pas, rappelons-le, de fichier centralisé des ressortissants français [2].

C'est par la possession d'un titre d'identité (carte d'identité ou passeport), délivré à travers une procédure codifiée, qu'un citoyen détient la preuve qu'il est bien le titulaire de son identité. En un sens, c'est la délivrance du titre d'identité qui « fixe » l'identité. Avant la délivrance du titre, un enfant, par exemple, est doté d'une forme embryonnaire d'identité, son inscription sur le registre d'état civil (dont il peut obtenir copie

1. Numéro d'inscription au registre national d'identification des personnes physiques (RNIPP).
2. Le Registre national d'identité des personnes physiques, qui est à la base du NIR, n'est pas un fichier des citoyens français. On y trouve également des étrangers.

sous la forme d'un extrait de naissance), son inscription dans le livret de famille ou sur le passeport des parents.

Le lien entre identité publique et titre d'identité n'est pas de même nature selon les pays. La carte d'identité n'existe pas dans tous les pays et n'est pas nécessairement obligatoire. La plupart des États européens, à l'exception notable du Royaume-Uni, ont cependant institué une carte d'identité, facultative ou non. Aux États-Unis, la carte de sécurité sociale et, surtout, le permis de conduire en sont progressivement venus à jouer le rôle de pièces d'identité officielles ; quelques États proposent une carte d'identité facultative.

La carte d'identité se distingue des autres pièces d'identité par la réunion de trois conditions :
– elle est délivrée par l'État ;
– elle vise des fins d'identification générale et non des usages spécifiques (comme le permis de conduire ou le passeport) ;
– elle contient des renseignements qui, en comparaison des autres pièces d'identité, en font un document privilégié pour identifier les personnes.

Le ministère de l'Intérieur envisage aujourd'hui une triple évolution de l'identité publique, à l'occasion du renouvellement des chaînes de production de la carte d'identité qui doit intervenir dans les années à venir : la procédure de délivrance des titres d'identité, la numérisation de la carte d'identité et, à l'occasion de cette numérisation, l'adjonction d'une fonction de signature électronique.

Nouvelle procédure : le titre fondateur

Le ministère de l'Intérieur a le projet de rendre plus sûre la procédure de délivrance des titres d'identité. La nouvelle procédure a été baptisée « titre fondateur » dans la mesure où elle permettrait la délivrance de la carte nationale d'identité et du passeport et autoriserait ensuite, dans des conditions simplifiées par rapport à la situation actuelle, l'accès à d'autres titres ou à d'autres prestations administratives.

En sécurisant cette procédure, l'État se donnerait les moyens de mieux garantir l'identité des citoyens français (la situation actuelle n'étant de ce point de vue pas entièrement satisfaisante : on en prend la mesure dans les cas d'usurpation partielle ou totale de l'identité).

Une carte d'identité électronique

À cette occasion, le ministère de l'Intérieur a engagé une réflexion sur la possibilité de doter la carte d'identité d'une puce électronique et de pouvoir délivrer, à terme, une gamme plus ouverte de titres, adaptée aux besoins spécifiques des usagers :
– la carte nationale d'identité simple (CNIE) ;
– la carte nationale d'identité électronique ;
– la carte du citoyen (CNIE +carte électorale) ;
– la carte du conducteur (CNIE +droits de conduire) ;
– le passeport simple ;
– le passeport électronique.

Il appartiendrait à l'usager de choisir la nature du titre qu'il souhaite obtenir.

La carte nationale d'identité électronique se présenterait sous la forme d'une carte de type carte bancaire. Le microprocesseur contiendrait les éléments évolutifs de l'identité (l'adresse par exemple), ceux dont la lecture constitue une atteinte à la vie privée (le sexe), des éléments de sécurisation de la carte (empreinte digitale, par exemple) et les applications nécessaires à l'authentification et à la signature électronique de son titulaire. Le titulaire pourrait, en utilisant un code PIN, accéder aux informations détenues dans le microprocesseur par des bornes interactives installées dans les services administratifs et pourrait exercer directement son droit de correction.

La carte électronique pourrait intégrer d'autres fonctions comme la carte électorale (ce qui permettrait de voter électroniquement) ou les droits de conduire (permis de conduire). Elle pourrait aussi intégrer une fonction de signature électronique qui permettrait d'accéder aux téléservices publics qui nécessitent une authentification, depuis un ordinateur ou sur des bornes.

Plusieurs pays européens ont entrepris de mettre en place une carte d'identité électronique. C'est le cas de la Finlande et de la Suède (ou la carte d'identité électronique est déjà opérationnelle), de l'Italie (où la carte électronique est en phase pilote), de la Belgique, l'Espagne et le Portugal, qui ont pris la décision de créer une telle carte. Une étude de faisabilité est en cours aux Pays-Bas. D'une manière ou d'une autre, les pays qui s'engagent dans cette voie retiennent l'option d'une carte multifonctionnelle (carte d'identité, d'électeur, d'assuré social) mais n'y intègrent pas nécessairement de fonction de signature électronique.

Chapitre 4

Vers l'administration électronique

L'informatique administrative des années soixante-dix était une informatique de production, orientée vers les besoins propres des administrations. Aux objectifs d'efficacité administrative se mêlaient, de manière confuse, des objectifs de « contrôle social ».

Au cours des années quatre-vingt, les administrations ont amorcé une modernisation qui visait à modifier les relations entre administrations et administrés. Les mots clefs de cette modernisation furent transparence administrative (les lois du 17 juillet 1978 sur la liberté d'accès aux documents administratifs ; celle du 6 janvier 1978 sur l'informatique, les fichiers et les libertés ; du 3 janvier 1979 sur les archives en 1979), simplification, télématique administrative, droits des usagers dans leurs relations avec les administrations, etc.

L'administration électronique s'inscrit dans cette filiation : elle se donne comme finalité première l'amélioration des services rendus au public.

Quelle administration électronique ?

Le relevé de décision du Comité interministériel de l'État du 15 novembre en trace les grandes lignes :
« L'État se donne pour objectif que soient proposées en ligne, d'ici à 2005, l'ensemble des démarches administratives des particuliers, des associations et des entreprises, ainsi que les paiements fiscaux et sociaux. Il s'agit de faire progressivement en sorte que chaque usager bénéficie des technologies de l'information et de la communication dans les transactions avec les services publics et puisse notamment :
– accéder simplement et rapidement à toutes les informations et à une aide personnalisée sur les services publics et ses démarches administratives. Un téléservice ne doit donc jamais être plus complexe à utiliser que son équivalent « papier » ;

– effectuer en ligne et de manière sûre toutes ses démarches avec les services publics sauf celles qui, par nature, exigent un déplacement. Cela inclut notamment les échanges eux-mêmes, mais également le suivi de ses dossiers, la définition de calendriers prévisionnels personnalisés, la relance par courrier électronique, etc. ;
– accéder à ses démarches passées et stocker en ligne, à son gré et en toute sécurité, les résultats dématérialisés issus de ces dernières ;
– exercer en ligne son droit d'accès et, le cas échéant, de modification des informations le concernant détenues ou échangées par les administrations, notamment aux dispositions de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. »

Des services intelligents

Un téléservice [1] est un service intelligent. Quand l'usager saisit un formulaire numérique, le système effectue un contrôle de ce champ. Par exemple, il s'assure qu'une date est saisie avec des chiffres et non avec des lettres, ou qu'une valeur se situe bien entre 1 et 100 s'il est prévu qu'elle ne saurait excéder 100. Ce contrôle s'effectue, de surcroît, en temps réel. L'usager n'a pas besoin d'aller jusqu'au bout du formulaire pour se rendre compte qu'il a commis une erreur.

Plus radicalement, les téléservices intelligents inversent les flux d'information entre usagers et administrations. Dans les démarches administratives traditionnelles, l'usager est tenu de donner des informations : l'administration se contente de vérifier les informations communiquées par les usagers. Une fois ces informations vérifiées, recoupées avec les informations que l'administration détient déjà, elle donne suite à la demande, instruit le dossier, déclenche une procédure qui donnera lieu, le cas échéant, à de nouvelles questions et transmissions d'informations.

Dans les téléservices avancés, l'administration communique les informations qu'elle détient : il revient à l'usager d'en vérifier la pertinence, de les compléter, de les actualiser ou de les corriger.

Des services personnalisés : la consultation du « compte »

En proposant l'accès à un « compte administratif personnalisé », éventuellement à plusieurs comptes (fiscal, social, etc.), l'administration ne fait pas autre chose que d'offrir un ensemble de facilités que les banques ou les entreprises de services et, parmi elles, des opérateurs de service public comme EDF, proposent d'ores et déjà.

En accédant à son compte, l'usager exercera, *de facto*, son droit d'accès à une partie des informations le concernant, détenues ou échangées par les administrations et, le cas échéant, son droit de modification.

1. La notion de téléservice, mieux que celle, datée, de téléprocédure, met l'accent sur le service que l'administration cherche à rendre.

Cette ouverture des systèmes d'information publics ne va pas sans difficultés. Ainsi, pour mettre en place le compte fiscal simplifié, le ministère des Finances et de l'Industrie a dû engager une refonte complète de son système d'information. Avec le projet Copernic, les systèmes d'information de la direction générale des Impôts, structurés et stratifiés chacun autour d'un impôt (logique métier) se restructurent progressivement autour du « client » afin de prendre en compte, quel que soit l'impôt, le foyer fiscal, et, au-delà, la personne elle-même.

La généralisation des téléservices et des « comptes » implique que bon nombre des systèmes d'information administratifs, conçus pour gérer des « procédures » se recentrent autour des bénéficiaires et des individus.

Des services qui s'inscrivent dans la durée : le dossier

Les démarches administratives se déploient dans le temps. Elles sont faites de correspondances qui s'échangent, de formulaires et de pièces qui sont demandés et transmis. Elles sont régies par des délais et des obligations, qui s'imposent soit à l'usager, soit à l'administration.

Les administrations se sont organisées, de tout temps, pour conserver une trace de tous ces flux de documents : elles tiennent à jour des dossiers. Symétriquement, pour certaines procédures, l'usager est tenu de conserver, pendant une certaine période, une trace des mêmes échanges. Il arrive également que l'administration refuse de délivrer des « duplicata » (c'est, par exemple, le cas des diplômes).

Les projets d'administration électronique se donnent l'ambition de transposer, dans l'univers numérique, cette notion de « dossier ». Le dossier ne se limite d'ailleurs pas à l'archivage des démarches passées et de leurs résultats ; il permet également de suivre (traçabilité) les différentes étapes d'une démarche en cours.

Des services transversaux aux différentes administrations

Pour l'illustrer, on prendra l'exemple d'un téléservice très simple et bien utile : la déclaration en ligne du changement d'adresse.

Aujourd'hui, il revient à l'usager de déclarer à chaque administration son changement d'adresse. On voit bien l'intérêt pour l'usager de pouvoir effectuer l'ensemble de ses déclarations en une seule fois et en ligne, à charge pour les administrations de d'organiser pour mettre à jour leurs bases de données. De la même manière, on voit bien l'intérêt pour les administrations d'être informées systématiquement du changement d'adresse d'un usager.

Pour mettre en place un tel service, il est bien sûr possible d'imaginer un scénario d'interconnexion des systèmes d'information qui

fasse par exemple que l'ensemble des administrations partagent un fichier d'adresse commun et unique, tenu à jour de manière centralisée. Un tel scénario semble cependant voué à rester théorique : il contreviendrait selon toute probabilité à la loi de 1978.

Heureusement, deux autres scénarios sont envisageables pour répondre au même besoin :
– scénario régulé : un service de télédéclaration du changement d'adresse qui repose sur un système d'échange ne conservant pas les adresses, sous le contrôle de la CNIL est mis en place. Cette dernière a contribué à définir des règles claires : les administrations qui seront destinataires de l'information, celles qui pourraient l'être, celles ne le seront en aucun cas ;
– scénario d'autonomie : le service de télédéclaration présente des options. Il revient à l'usager de choisir quelles administrations seront informées de son changement d'adresse et lesquelles ne le seront pas. Il opérera ce choix en fonction d'avantages et d'inconvénients qu'il est le seul à pouvoir arbitrer.

Des téléservices publics ouverts et interopérables avec les téléservices privés

Les relations avec les services publics ne se réduisent pas au face à face usager-administration. La fourniture de certaines prestations administratives repose sur un triangle État-usager-tiers privé. Pour certaines procédures, les usagers ainsi sont tenus de faire appel à un notaire, à un avocat ou à un architecte (permis de construire). Les banques sont un intermédiaire obligé pour les flux financiers entre administrations et usagers. Ces tiers sont parfois tenus au secret professionnel, comme l'avocat qui assiste le justiciable dans ses rapports avec la justice. Parfois, c'est le service public lui-même qui est délégué à un officier ministériel, au statut hybride.

Et, bien entendu, certains téléservices sont distribués par des opérateurs privés : les concessionnaires automobiles assurent ainsi, pour le compte de leurs clients, l'interface avec les préfectures pour l'obtention des cartes grises.

Les téléservices publics devront donc s'interfacer avec les téléservices privés. À terme, le compte fiscal pourrait ainsi être articulé avec le téléservice bancaire du contribuable pour globaliser et automatiser les opérations de paiement. Le compte fiscal pourrait par exemple permettre au contribuable d'ajouter électroniquement, dans sa déclaration de revenus, les données issues de sa banque, voire directement de son employeur.

De même, on peut imaginer que le téléservice de déclaration du changement d'adresse serait ouvert à des opérateurs privés : compagnies de téléphone, d'électricité, banques, etc.

Cette imbrication entre téléservices publics et téléservices privés est particulièrement marquée pour tout ce qui touche à l'authentification et à la gestion des identités numériques.

À l'horizon, la dissociation de la production et de la distribution des services (guichet polyvalent)

L'administration électronique s'assigne l'objectif de présenter un guichet polyvalent unique à chaque usager, masquant la complexité des traitements aboutissant à la délivrance des droits. Les Anglo-Saxons parlent d'administration *uni-face*, uni-visage.

La mise en place de portails (comme service-public.fr) est une première étape dans cette unification du *« front office »* des administrations. Ces portails gouvernementaux permettent d'accéder aux services de l'ensemble des administrations. Service-public.fr va plus loin et propose un guide des droits et démarches composé de fiches pédagogiques qui orientent ensuite l'usager vers l'administration concernée ou la téléprocédure elle-même.

Les projets de « compte administratif personnalisé » s'articulent explicitement sur l'existence d'un portail. Dès lors que le portail unifie l'accès à l'ensemble des services des administrations, et qu'il intègre de plus en plus de fonctionnalités techniques (identification-authentification, paiement, conservation d'une trace de toutes les démarches à travers un ou des dossiers), le portail tend à devenir le *front office* pour l'ensemble des administrations.

Les portails, les centres d'appels, les dispositifs d'accès au compte administratif personnalisé vont progressivement prendre en charge et absorber la fonction de distribution pour le compte des administrations spécialisées. Celles-ci, progressivement libérées du contact direct avec l'usager, pourraient se concentrer exclusivement sur les activités de production des services (analyse des dossiers, décision, exécution).

Cette évolution s'observe d'ores et déjà dans la sphère de la protection sociale avec Net-Entreprises. Conçu comme un portail qui permet d'effectuer l'ensemble des déclarations sociales, Net-Entreprises est bien le *« front office »* des quinze organismes nationaux ou fédérations du monde de la protection sociale, chacun de ceux-ci continuant à assurer la gestion de ses prestations en s'appuyant sur le canal de distribution et d'interaction avec l'usager que constitue le site Net-Entreprises.

À l'horizon, par rétroaction des processus sur les structures, on peut imaginer que les différents services qui assurent la distribution des services de l'administration (portail, centres d'appels, interlocuteurs polyvalents, voire une partie des guichets physiques), soient complètement externalisés et regroupés au sein d'une entité publique unique ou de plusieurs entités. C'est d'ailleurs, au niveau local, cette philosophie qui inspire d'ores et déjà les Maisons des services publics.

Au terme de ce processus, c'est un ré-agencement des services de l'État qui se profile autour de trois pôles, trois figures de l'administration :
– l'État régalien : fondé sur le principe de souveraineté, il a l'autorité pour prescrire, imposer, taxer, prélever, interdire et sanctionner ;

– la production des services publics : les administrations assureraient la production des prestations administratives – politiques publiques, gestion des droits, gestion des procédures – en se dégageant de leur distribution. Pour produire plus efficacement ces prestations, elles se réorganiseraient autour des systèmes d'information métiers ;
– une ou plusieurs entités publiques spécialisées dans la distribution, en ligne ou par tout autre moyen, des services publics : orientée(s) vers l'usager, elles assurent l'interface entre l'usager et les administrations productrices.

Administration électronique en France : où en sommes-nous ?

La France avait été, avec le minitel, pionnière en matière d'administration électronique. Au début des années quatre-vingt-dix, elle hésite à basculer ses services sur internet, puis s'y résout progressivement à partir de 1996. En août 1997, le Premier ministre décide la migration des services de l'État du minitel vers l'internet. En 1998, le gouvernement place l'administration électronique parmi les six chantiers prioritaires du programme d'action gouvernemental pour l'entrée de la France dans la « société de l'information » (PAGSI).

Depuis lors, la présence en ligne des services publics n'a fait que croître. On recensait, en février 2002, 4 700 sites internet publics. 1 123 formulaires administratifs sont en ligne, soit environ 65 % des formulaires administratifs existants. Ils représentent la totalité des formulaires les plus courants pour les particuliers et les entreprises. 131 téléservices (des services de l'État, des organismes de sécurité sociale et des collectivités locales) sont accessibles en ligne. Ils concernent les particuliers (80 %) comme les entreprises (20 %) et portent sur l'obtention de documents d'état civil, la gestion des impôts, la recherche d'emploi, les aides aux entreprises, les déclarations sociales, ou les marchés publics.

Ce mouvement vers les téléservices s'accentue : plus d'un tiers des webmestres publics de l'État déclarait développer des téléprocédures en 2001, notamment dans les domaines de la prise de rendez-vous, des inscriptions en ligne et des démarches administratives [1].

Le portail de l'administration, service-public.fr, a reçu près d'un million de visites en février 2002 (47,5 millions de pages vues entre décembre 2000 et décembre 2001). Les 3 000 courriers électroniques qui lui sont adressés chaque mois reçoivent une réponse dans les 48 heures. Avec service-public.fr, la France est parvenue, en un temps assez bref, à bâtir un portail gouvernemental efficace et très complet [2].

1. Enquête annuelle sur le web public de la DIRE.
2. Elle tirait parti des acquis de l'expérience et du savoir-faire de La Documentation française (en coopération avec l'ensemble des administrations) dans la mise en place de « portails » télématiques comme 3615 Admitel ou 3615 Vosdroits.

En 2001, 2,5 millions de personnes ont calculé leur impôt sur le site de l'administration fiscale. Les principales déclarations sociales (déclaration unique d'embauche ; déclaration annuelle de données sociales ; contribution sociale de solidarité des sociétés avec possibilité de télérèglement pour la campagne 2002 ; déclaration unifiée de cotisations sociales) sont désormais entièrement gérables en ligne sur le portail Net-Entreprises. Près de 400 000 entreprises y sont inscrites, dont 7 000 cabinets d'experts-comptables.

SESAM-Vitale constitue aujourd'hui la téléprocédure la plus importante au monde : 1,5 million de feuilles de soins électroniques sont produites par jour, soit un tiers du total de l'ensemble des feuilles de soins, moins de quatre ans après la distribution de la première carte Vitale.

Au sein des administrations également, l'usage des TIC progresse : 85 % des postes de travail de l'État (hors enseignement et armées) disposent d'un ordinateur ; plus de la moitié d'entre eux sont en réseau (local et/ou intranet). Plus de 30 % des postes sont connectés à internet.

La mise en réseau des services de l'État se développe à travers AdER (Administration en réseau), un « intranet global » interadministration. Au niveau local, des systèmes d'information territoriaux (SIT) sont en place dans la totalité des départements métropolitains et en cours de généralisation dans les DOM-TOM.

Si certains téléservices ont pu être mis en place sans modification des organisations, des méthodes de travail et des systèmes d'information, le déploiement de services pleinement interactifs et personnalisés implique une réingéniérie des processus et une refonte des systèmes d'information.

Selon Thierry Carcenac [1] *« la première étape est réalisée : il s'agissait la mise en place d'un site portail et d'outils de messagerie électronique, d'information ou d'échange.*
« La deuxième étape est planifiée pour l'année 2001 : la mise en place de téléprocédures [2], sans modification importante des processus de traitement des données télétransmises.
« La troisième étape, intermédiaire mais capitale, sera de profiter des potentialités offertes par les réseaux pour redéfinir, en profondeur, les processus et les traitements de données au sein de l'administration. Cette étape fera vraisemblablement apparaître les avantages d'une nouvelle configuration du travail centrée sur la transversalité et le travail en équipe, afin de pouvoir répondre de manière rapide et personnalisée aux attentes du public – et aux besoins des administrations.
« Une fois cette étape intermédiaire réalisée (et il ne faut pas sous-estimer la difficulté de sa mise en œuvre), l'on pourra la généraliser d'une

1. Thierry Carcenac, *Pour une administration électronique citoyenne*, La Documentation française, 2001.
2. Une téléprocédure se définit comme un échange dématérialisé de formalité entre une autorité publique et ses partenaires et usagers. Le terme de téléprocédure recouvre plusieurs acceptions dont l'objectif ultime est de parvenir à supprimer totalement la phase » papier « .

transversalité à l'intérieur d'une administration centrale à une véritable transversalité entre les administrations. »

Où en sont nos partenaires internationaux ?

La notion d'administration électronique a surgi dans les années quatre-vingt quand une fraction significative de la population a commencé à détenir des micro-ordinateurs ou des terminaux télématiques. Elle a pris véritablement son essor avec l'apparition de cette nouvelle infrastructure, à la fois mondiale, ouverte et largement standardisée qu'est internet. En 1992, le vice-président américain Al Gore appelle l'administration américaine à se réinventer à travers le *« e-government »*. Très vite, d'autres pays (Suède, Finlande, Singapour, Grande-Bretagne) reprennent cette perspective à leur compte. À l'heure actuelle, tous les gouvernements de l'Union européenne ont mis en œuvre des programmes de développement de l'administration électronique, consolidés au sein du programme « e-Europe ».

Nos principaux partenaires ont, pour la plupart, franchi comme nous la première étape décrite par Thierry Carcenac, celle de l'ouverture de sites informant l'usager des compétences et des attributions des administrations, et la deuxième, qui consiste à proposer des services interactifs sur des sites dynamiques : formulaires intelligents et téléprocédures simples. Beaucoup ont créé un site portail qui donne accès à tout ou partie des services en ligne des administrations.

Plusieurs gouvernements se dont donné le même horizon, l'année 2005, pour la généralisation des téléservices. Considérant qu'ils ont réalisé les deux premières étapes (services d'information et services interactifs), largement engagé la troisième (transactions), ils amorcent désormais la transformation de leurs procédures internes et de leurs systèmes d'information métiers pour offrir des services « intégrés » et personnalisés.

Ainsi, avec le *Public Services Broker*, le gouvernement irlandais met le cap sur l'intégration des services. On y trouve un service d'authentification et un contrôle d'accès, un espace de stockage sécurisé (de type « coffre-fort »), la possibilité de stocker et de réutiliser des données personnelles, un suivi des dossiers, ainsi qu'un regroupement des services par type d'événement ou par thème. Le service d'authentification doit être basé sur l'utilisation conjointe d'un identifiant, le *personal public service number* (utilisé depuis de nombreuses années pour les services d'imposition et d'assurance sociale) et d'une carte, la *social services card*. Il est envisagé de créer une « famille » de cartes électroniques adaptées aux besoins de différents groupes d'utilisateurs. Au niveau de base, la carte et un code confidentiel pourraient être suffisants pour accéder à certains services ; là où un haut niveau de sécurité est requis, une des technologies

possibles pourrait être l'utilisation de signatures électroniques et de certificats dans le cadre d'une infrastructure à clefs publiques [1].

Le gouvernement québécois, pour sa part, travaille à la mise en œuvre de « prestations électroniques de services » (PES) [2]. L'idée force, ce sont les « grappes de services » : une prestation intégrée de services évitant à l'usager de subir les désagréments dus aux cloisonnements au sein et entre les administrations. La mise en œuvre d'une grappe de services s'appuie sur un guichet unique ; des solutions technologiques offrant des modes d'accès diversifiés (guichet, téléphone, internet) sont mises en place. Les citoyens québécois ont accès aujourd'hui à sept grappes de services, toutes accessibles à partir du portail gouvernemental : parmi elles, on citera notamment le changement d'adresse [3] et la déclaration de perte ou de vol de documents d'identité ou de cartes [4].

Le gouvernement suédois fonde ses espoirs sur le *Government eLink* : ici, l'accent est placé sur la fourniture conjointe de services par différentes agences gouvernementales et par le secteur privé. *Government eLink* ne doit nécessiter aucune interface humaine dans les agences. Sont d'ores et déjà opérationnels : la transmission d'enregistrements entre le Conseil national des impôts et le Conseil national de l'assurance ; la télédéclaration d'impôt des sociétés ; la transmission des feuilles de soins.

Outre-Manche, la *Government Gateway* est une étape dans la stratégie du gouvernement britannique : elle devrait à terme aboutir à un guichet unique sécurisé en ligne. Après une phase d'inscription préalable, l'usager (ainsi que les personnes qu'il désigne) pourra accéder à de nombreux services en lignes au travers d'un point d'entrée unique sécurisé [5]. Pour s'inscrire, il est nécessaire de disposer au préalable, d'un certificat numérique [6]. La *Gateway* est opérationnelle depuis mars 2001 pour la télédéclaration de TVA, les demandes d'aide (dans le cadre de la politique agricole commune) auprès du ministère de l'Agriculture, de la Pêche et de l'Alimentation [7] et les déclarations de revenus. Comme en Suède, l'accent est mis sur les partenariats avec le secteur privé.

À travers ces quelques exemples, on voit converger les choix de nos partenaires sur les grandes options : mise en réseau des administrations, partage des informations entre les administrations (qui s'étend, selon les pays, aux collectivités territoriales et aux organismes sociaux), accès

1. La première version du portail, Oasis, a été ouverte en mai 2001, et permet d'accéder aux informations concernant les services destinés aux citoyens (http://www.oasis.gov.ie).
2. http://www.atica.pm.gouv.fr/dossiers/documents/Irlande.shtml et http://www.atica.pm.gouv.fr/dossiers/documents/grappes_Quebec.shtml.
3. http://www.changer-adresse.info.gouv.qc.ca/fr/index.asp.
4. http://www.perte-cartes.info.gouv.qc.ca/fr/index.asp.
5. http://www.atica.pm.gouv.fr/dossiers/documents/gateway.shtml.
6. Le pilotage est effectué par l'équipe du *« e-Envoy »* rattaché aux services du Premier ministre. Y participent notamment la direction générale des impôts (*Inland Revenue*), l'administration des douanes et des contributions indirectes (*HM Customs & Excise*) et le ministère de l'Agriculture, de la Pêche et de l'Alimentation (*Ministry of Agriculture, Food and Fisheries*).
7. http://www.maff.gov.uk/ebus/eforms/iacsaaps/iacsaaps.htm.

personnalisé des citoyens et des entreprises à travers des guichets d'accueil polyvalents en ligne, personnalisation des services (ce qui suppose une identification de la personne), recours, à un terme pas toujours facile à déterminer, à des certificats numériques afin de sécuriser les interactions avec les administrations.

Les méthodes de mise en œuvre reposent sur la mise en place d'infrastructures et de services communs, l'affichage de normes et de standards, la publication progressive de schémas de données communs (avec des différences : ainsi, la mise en œuvre du cadre d'interopérabilité présente un caractère plus ou moins obligatoire selon les pays et il est accompagné ou non de la mise en place d'éléments d'architecture matérielle et logicielle ou *middleware*).

Chapitre 5

Quelle protection des données personnelles pour l'administration électronique ?

Le déploiement des téléservices « intégrés » (communs à plusieurs administrations) et la mise en place d'un compte administratif personnalisé donnent lieu à de nouveaux flux de données personnelles, qui doivent être gérés dans le cadre juridique actuel de la protection de ces données.

Le cadre juridique et la jurisprudence de la CNIL

Les fichiers administratifs : un enjeu historique fondateur

La loi du 6 janvier 1978 trouve son origine dans la révélation au public de plusieurs projets concomitants de fichiers administratifs conduits de façon particulièrement peu transparente. Plus précisément, le projet Safari du ministère de l'Intérieur consistant à mettre en œuvre un ordinateur très puissant destiné à la centralisation des bases de donnée que possédaient les services de police s'ajoutait à la décision prise en 1970 par l'INSEE d'informatiser le Répertoire d'identification des Français pour parvenir à un identifiant unique de tous les Français. L'émotion suscitée par la révélation de ces projets avait conduit à la constitution d'une commission chargée de *« proposer au Gouvernement, dans un délai de six mois, des mesures tendant à garantir que le développement de l'informatique dans les secteurs public, semi-public et privé se réalisera dans le respect de la vie privée, des libertés individuelles et des libertés publiques »* (décret du 8 novembre 1974). Cette commission a remis le 27 juin 1974 un rapport sur la base duquel a été élaboré le projet de loi qui a abouti à la loi du 6 janvier 1978.

La loi du 6 janvier 1978 garde trace de cette sensibilité particulière aux traitements de données du secteur public :

– elle instaure un régime dissymétrique soumettant les fichiers publics à un régime d'autorisation préalable (article 16) et les fichiers privés à un simple régime de déclaration (article 15) ;
– elle soumet l'utilisation du Répertoire national d'identification des personnes physiques (RNIPP), géré par l'INSEE, à une autorisation par décret en Conseil d'État pris après avis de la CNIL (article 18).

Le futur cadre législatif : la révision, en cours, de la loi de 1978

La directive sur la protection des personnes à l'égard du traitement des données à caractère personnel (directive nº 96/46/CE du Parlement européen et du Conseil du 24 octobre 1995) est en cours de transposition.

Le projet de loi voté (en première lecture) à l'Assemblée nationale introduit en effet des amendements à la loi du 6 janvier 1978. Désormais, ce sera la finalité du « fichier » et la nature des données qu'il collecte qui détermineront le régime applicable, et notamment l'intervention préalable ou non de la CNIL, quelle que soit la nature publique ou privée de la personne qui le constitue. Le régime de droit commun est celui de la déclaration. Celle-ci sera simplifiée pour les catégories les plus courantes de « fichiers » répondant à des normes définies par la CNIL. Cette dernière pourra même dispenser de toute déclaration les traitements les plus anodins.

Les fichiers publics dont la création, quel que soit l'objet, résulte aujourd'hui d'un acte réglementaire pris après avis de la CNIL, seront désormais soumis soit au droit commun du régime déclaratif, soit au régime d'autorisation de la CNIL s'ils appartiennent à l'une des huit catégories énumérées à l'article 25 du projet [1]. Même pour ces fichiers, il ne sera plus exigé que l'avis de la CNIL soit conforme, comme c'est actuellement le cas pour les traitements de souveraineté ; en revanche, l'avis sera publié en même temps que le décret autorisant le traitement, de manière à ce que, le cas échéant, les observations ou les réserves de la Commission soient parfaitement connues.

À l'article 18 de la loi qui encadrait l'utilisation du NIR se substituerait un article 27 nouveau qui déterminera le régime particulier applicable aux traitements à finalité publique qui, soit incluent le numéro INSEE des personnes, soit portent sur la totalité ou la quasi-totalité de la population. La procédure s'inspire étroitement de celle instituée par le législateur de 1978 à l'article 18 du texte actuel, puisqu'elle repose sur une

1. Données dites sensibles, données génétiques, données relatives aux infractions ou aux condamnations, numéro d'inscription au Répertoire national d'identification des personnes physiques (NIR), appréciations sur les difficultés sociales des personnes, données biométriques nécessaires au contrôle de l'identité des personnes, données utilisées à des fins d'exclusion du bénéfice d'un droit, d'une prestation ou d'un contrat, dès lors que cette exclusion ne repose pas sur une condition légale ou réglementaire, et interconnexion entre des « fichiers » de nature différente.

autorisation du traitement par décret en Conseil d'État après avis motivé de la CNIL. Le texte instaure une garantie supplémentaire, puisqu'il exige que l'avis de la Commission soit publié. Une possibilité d'autorisation par arrêté sur avis de la CNIL est prévue si le traitement envisagé répond à certains critères dont la réunion est significative d'un moindre degré de risque au regard des droits et libertés des personnes. Cette procédure allégée a également vocation à s'appliquer aux traitements recourant à une consultation du RNIPP, sans que le numéro d'identification des personnes (NIR) soit inclus parmi les données traitées.

Si la nouvelle approche qui inspire la directive et sa transposition ne fait donc plus du caractère public des traitements de données un critère déterminant, elle continue donc à organiser un contrôle spécifique des fichiers publics qui recèlent des enjeux particuliers de protection de données.

Le NIR : un usage encadré

Le NIR, numéro d'inscription au RNIPP géré par l'INSEE, qui a été créé en 1941, est un numéro stable, permanent et fiable. À défaut d'un fichier central des nationaux ou des résidents, et du fait notamment de l'absence de centralisation de l'état civil, le RNIPP assure une fonction de certification de l'état civil, car il résout les cas d'homonymie. Mais les craintes liées au caractère signifiant du NIR, qui n'est pas aléatoire, mais qui donne des informations sur son détenteur, et le refus de voir l'identité de chacun réduite à un simple matricule, ont conduit à un encadrement strict de son utilisation. Ainsi, l'article 18 de la loi du 6 janvier 1978 dispose que : *« L'utilisation du Répertoire national d'identification des personnes physiques en vue d'effectuer des traitements nominatifs est autorisée par décret en Conseil d'État pris après avis de la Commission »*.

Cette disposition, qui vise l'utilisation du NIR dans les fichiers, n'interdit pas les demandes des administrations à l'INSEE afin de consulter le répertoire, à condition que l'administration demandeuse n'enregistre pas le NIR. Les administrations ont en effet la possibilité de demander à l'INSEE de consulter le répertoire pour se faire certifier l'état civil de leurs ressortissants. Les administrations (une trentaine en 1999) adressent à l'INSEE les données d'état civil des personnes présentes dans leurs fichiers, avec ou sans le NIR, selon qu'elles ont été ou non autorisées à l'enregistrer dans leurs bases, ce qui permet à l'institut après consultation du RNIPP de répondre s'il connaît ou non ces personnes. L'INSEE conserve en outre, pour chacune des personnes sur lesquelles il a été interrogé, les références de l'organisme qui l'a interrogé. La consultation n'implique pas l'enregistrement du NIR dans les fichiers soumis à cet examen. Une telle consultation du RNIPP est par exemple autorisée de longue date par la CNIL pour les administrations fiscales à des fins de contrôle de l'état civil, à condition que le NIR ne soit pas mémorisé (délibération du 18 décembre 1984). Mais de nombreuses administrations souhaiteraient aller plus loin et pouvoir conserver le NIR pour en faire l'identifiant de référence de leurs fichiers.

La collecte et l'enregistrement du NIR ont été cantonnés par la jurisprudence de la CNIL et se trouvent essentiellement limités à la sphère sociale.

La délibération de la CNIL du 29 novembre 1983 constate que le NIR est devenu *« l'instrument de référence fondamental de l'état civil en France, destiné en particulier à lever le doute sur les homonymies »* et qu'il a été utilisé d'emblée par la sécurité sociale, ce qui constitue une *« extension de finalité du numéro »* impossible à remettre en cause *« sauf à entraîner de graves perturbations dans le fonctionnement du régime de protection sociale »*. Admettant donc par force cette utilisation du NIR, la CNIL souligne le risque, en raison du caractère signifiant des chiffres le composant, de voir le NIR se généraliser et devenir l'identifiant national. Elle relève que *« la tendance à la généralisation du NIR ne saurait être justifiée ni par les nécessités de résoudre les difficultés s'attachant à la conception des traitements, ni par le souci de faciliter les interconnexions de fichiers que le législateur a au contraire voulu limiter »*. Elle recommande que *« les responsables de la conception d'applications informatiques se dotent d'identifiants diversifiés et adaptés à leurs besoins propres »*. Cette délibération distingue donc avec soin deux fonctions, certification de l'état civil d'une part et gestion des fichiers de personnes d'autre part.

• En dehors du domaine social, aussi largement entendu soit-il, la CNIL a œuvré à l'adoption par les administrations d'identifiants qui leur soient propres, ce qu'ont fait par exemple l'Éducation nationale (Numen) et l'administration fiscale (numéro dit SPI, Simplification des procédures d'imposition).

• L'article 107 de la loi de finances pour 1999 a ouvert aux administrations fiscales l'utilisation du NIR dans un cadre restrictif qui a été précisé à la fois par le législateur, par le Conseil constitutionnel et par deux décrets en Conseil d'État pris après avis de la CNIL.

L'interconnexion de fichiers : une pratique réglementée

L'interconnexion n'est pas en soi une pratique interdite, ni par la loi ni par la CNIL, mais elle est sévèrement encadrée. Elle est assimilée à un véritable traitement qui doit, en tant que tel, être subordonné à l'avis de la Commission (article 5 de la loi du 6 janvier 1978).

L'avis de la CNIL sur tout projet d'interconnexion prend en compte plusieurs exigences :
– saisie d'un projet d'interconnexion entre fichiers, la CNIL s'assure en premier lieu que l'échange d'information peut légalement avoir lieu. Ce n'est pas le cas quand les informations sont protégées par le secret professionnel ou par un secret particulier (médical, bancaire, fiscal, statistique), à moins que ce secret ne soit levé par la loi ;
– l'interconnexion doit répondre aux grands principes qui régissent les fichiers, et notamment à l'exigence de données *« adéquates, pertinentes et*

non excessives » (article 5c de la convention nº 180 du Conseil de l'Europe). Elle doit ainsi être proportionnée au regard des objectifs poursuivis, et les informations mises en relation doivent être pertinentes. La liste des bénéficiaires des nouveaux circuits d'information est contrôlée ;
– l'interconnexion doit être portée à la connaissance des personnes intéressées ;
– l'interconnexion ne peut donc s'effectuer en utilisant le NIR que si les deux administrations sont autorisées à l'utiliser chacune pour ses propres fichiers et à procéder entre elles à des échanges d'informations sous les garanties exposées plus haut.

Compte tenu de cette jurisprudence de la CNIL, les interconnexions qui ont été autorisées sont assez limitées.

Ces interconnexions sont de surcroît le plus souvent autorisées par la loi, dont l'intervention est nécessaire pour lever le secret qui couvre les informations partagées. Elles se justifient généralement par un impératif de contrôle de l'utilisation des fonds publics. C'est dans le domaine social que se rencontrent la plupart de ces interconnexions.

Contrôle social ou amélioration service rendu au public ?

La loi de 1978 et, au-delà, le corpus de règles édictées par la CNIL sont à l'évidence contraignants.

Ces règles sont d'autant plus rigoureuses que la CNIL a dû, tout au long des années 1980 et 1990, batailler avec les administrations autour de traitements publics insuffisamment soucieux de protection de la vie privée.

Plutôt que d'opposer un avis défavorable aux projets qu'elle estimait critiquables, la CNIL a pris l'habitude de rendre des avis favorables mais assortis de réserves. *« Face à un avis de la CNIL comportant des réserves, l'administration est placée devant une alternative : soit elle fait siennes les réserves de la Commission en les intégrant dans le texte de création du traitement, soit elle entend les écarter et alors elle doit susciter un avis conforme du Conseil d'État »* [1]. Dans la quasi-totalité des cas, les administrations préfèrent se soumettre et prendre en compte les réserves de la Commission.

Comme l'observe Herbert Maisl, *« jusqu'à présent, la CNIL a surtout eu à se prononcer sur des traitements publics dont la création était, d'abord, justifiée dans l'intérêt général par un meilleur fonctionnement de l'État davantage que par un service de meilleure qualité à rendre*

1. Herbert Maisl, « Changer la CNIL ? Pour quoi faire ? », *Expertises*, nº 200, 1996.

à l'usager ; dans une perspective, par exemple, de lutte contre la fraude ou contre l'insécurité ».

Très sourcilleuse face aux traitements publics qui contribuent à une forme de contrôle social, la CNIL a souvent regretté que les projets qui lui étaient soumis prennent insuffisamment en compte des objectifs de simplification au profit, cette fois, du public. Il lui est arrivé de suggérer aux administrations de modifier certains projets dans ce sens.

Le président de la CNIL, Monsieur Gentot, et son vice-président, Marcel Pinet, ont rappelé, en de nombreuses occasions, que *« le développement des téléservices, dès lors qu'ils peuvent permettre de simplifier les démarches administratives et de rapprocher le citoyen de son administration, ne peut que rencontrer la faveur de la CNIL »*. La CNIL propose ainsi sur son site une procédure de télédéclaration des sites web.

La loi et la CNIL ne font pas obstacle aux téléservices

Depuis 1997, la Commission s'est prononcée sur un certain nombre de téléprocédures : télédéclarations sociales par les entreprises, télétransmission des feuilles de soins ; télédéclarations de revenus, télérèglement des impôts ; télédéclaration de la TVA ; délivrance par internet de certains extraits du casier judiciaire.

Elle a eu à se prononcer également sur des projets de téléservices dans les collectivités locales : inscription en ligne dans les établissements scolaires, délivrance de fiches d'état civil, prise de rendez-vous avec les services municipaux, etc.

De l'ensemble des avis rendus se dégage un « cahier des charges » des téléservices en cinq points.

L'identification de l'usager

La consultation en ligne du compte peut s'effectuer selon les dispositifs d'identification spécifiques aux systèmes d'information de chaque service public concerné (et acceptés par la CNIL), que l'usager a l'habitude d'utiliser dans le cadre de ses relations « traditionnelles » avec chacun de ces services. C'est le cas, par exemple, du matricule allocataire pour la consultation du compte prestations tenu par la caisse d'allocations familiales ; du numéro de sécurité sociale pour l'accès à son compte retraite (service proposé par la CNAVTS) ; du numéro SPI pour la consultation de son compte fiscal ; du numéro d'identification du demandeur d'emploi (GIDE 1 bis) pour le dépôt de sa demande sur le site de l'ANPE.

S'agissant des télédéclarations, la CNIL a adopté le même raisonnement à l'exception toutefois de la télédéclaration de revenus,

procédure pour laquelle elle a estimé préférable de recommander l'usage d'un identifiant spécifique, annuel, non signifiant, plutôt que le numéro FIP (numéro de foyer fiscal), numéro non confidentiel car porté notamment sur les avis d'imposition, document susceptible d'être communiqué à des tiers (organismes sociaux, bailleurs).

L'authentification des usagers

Cette authentification peut s'effectuer par confrontation des informations communiquées par l'intéressé et des données concernant celui-ci détenues par l'organisme dans ses fichiers.

Le recours aux procédés de signature électronique

Avant même la reconnaissance juridique de la signature électronique, la CNIL s'était prononcée favorablement, en 1998, sur l'utilisation de la carte du professionnel de santé, pour signer, de façon électronique, les feuilles de soins télétransmises aux caisses de sécurité sociale [1]. Elle a fortement recommandé l'utilisation de la signature électronique pour la mise en œuvre des télédéclarations fiscales [2].

Le recours systématique à des procédés de signature électronique ne constitue pas cependant aujourd'hui, pour la CNIL, une condition préalable à la mise en place des téléprocédures.

La plupart des téléservices publics mis en œuvre actuellement reposent sur des dispositifs d'identification et d'authentification « classiques » reposant sur un code d'identification (qui peut être le numéro d'identification attribué par l'organisme) et un mot de passe, généralement adressé sous pli confidentiel et que l'usager peut changer à sa guise.

Le recours aux procédés de chiffrement pour assurer la confidentialité des données

Le recours à des moyens de chiffrement (cryptage) pour assurer la confidentialité des données constitue, pour la CNIL, un impératif dès lors qu'il s'agit de transmettre par des réseaux ouverts de type internet des informations sensibles telles que des données de santé ou des données financières. La libéralisation, en France, de l'utilisation des moyens de

1. Délibération du 13 janvier 1998 portant avis sur un projet de décret relatif à la carte de professionnel de santé.
2. Ainsi, dans l'avis rendu le 3 février 2000 sur la télédéclaration d'impôt sur le revenu, la CNIL a-t-elle demandé que l'administration fiscale étudie un renforcement des dispositifs de sécurité incluant la mise en place d'un procédé de signature électronique (devant d'ailleurs conduire à ce que chaque époux puisse disposer d'une signature électronique). Cette demande a été réaffirmée lors de l'avis du 8 février 2001.

cryptologie a peu à peu permis à la CNIL de renforcer ses exigences en la matière.

Elle estimait, dès 1997, que les données de santé, confidentielles par nature, devaient surtout si elles sont appelées à circuler sur internet bénéficier de mesures de protection particulières, leur chiffrement par algorithme de cryptage constituant à cet égard l'une des seules garanties réellement efficaces.

Dans le domaine social, lors de la mise en place, par la CNAMTS, du codage des actes de biologie [1] appelés à être télétransmis aux caisses de sécurité sociale par les professionnels de santé, elle considérait *« qu'eu égard aux risques de divulgation et d'utilisation détournée des informations, la CNAMTS* [devait] *examiner les modalités qui pourraient être mises en œuvre afin de chiffrer les données d'identification des assurés »*. Une exigence qu'elle a réitérée à propos du codage des médicaments et à l'occasion de la généralisation du dispositif SESAM-Vitale.

À propos des télédéclarations tant sociales (TDS NET) que fiscales (télédéclarations de revenus), la Commission a estimé que des dispositifs de chiffrement devaient être instaurés dès lors que le recours à la téléprocédure revêtait un caractère obligatoire.

Information et droit d'accès

La dématérialisation des procédures administratives doit, selon la CNIL, s'accompagner d'une information claire des usagers leur permettant tout à la fois de s'assurer de la sécurité juridique du dispositif qui leur est proposé et de continuer à exercer les droits qui leur sont notamment reconnus par la loi du 6 janvier 1978. Ainsi, lors des différents avis rendus sur les téléprocédures fiscales, la CNIL a insisté sur la nécessité d'informer clairement les contribuables sur les conditions d'adhésion à ces téléprocédures et en particulier sur les mesures de sécurité adoptées, les modalités d'accusé réception, les conditions d'exercice du droit d'accès et de rectification, la nécessaire conservation d'une copie papier de l'envoi dématérialisé.

Dans le domaine social, la Commission a également rappelé que l'assuré devait pouvoir obtenir du professionnel de santé une copie papier de la feuille de soins électronique transmise.

De cet examen des recommandations ou des conditions posées par la CNIL, il ressort que la CNIL ne freine en aucune façon le développement des téléprocédures. Il convient d'ajouter, cependant, que la vigilance de la CNIL à l'égard des interconnexions et des identifiants tend à cantonner les téléprocédures dans le périmètre de chaque ministère ou, s'agissant de téléservices communs à plusieurs administrations ou organismes de service public, à l'intérieur de « sphères » déjà structurées. La délimitation de ces sphères repose sur l'utilisation d'un identifiant commun, comme le NIR, pour la sphère sociale, ou le Numen, pour la sphère éducative.

1. Avis du 19 décembre 1995 sur la mise en place, par la CNAMTS, du codage des actes de biologie.

Deuxième partie

Idées directrices

Les administrations et le public : un pacte de confiance à renégocier

Accès unifié à travers un portail et un compte, services intelligents, personnalisés, communs aux différentes administrations, systèmes ouverts et interopérables avec les téléservices privés, circulation plus fluide des données entre administrations : tels sont les caractères de l'administration électronique à venir. Telles sont aussi les conditions d'une amélioration tangible des services qu'elle rend. Sa mise en œuvre suppose donc une réévaluation du compromis conclu en 1978 qui régit les relations entre les administrations et le public.

Face à la défiance qu'inspirait alors l'informatique d'État, la loi de 1978 a strictement limité la connaissance que les services de l'État avaient et risquaient d'acquérir sur les personnes. Une autorité indépendante, la CNIL, a été spécialement instituée pour y veiller. La loi a strictement limité les échanges de données entre administrations. Bernard Tricot, auteur du projet de loi « informatique et libertés », décrit ce cloisonnement comme un choix conscient en faveur des libertés publiques. *« On entend dire souvent qu'il est temps de désenclaver les différents services de l'administration par la diffusion et l'échange des informations.* (...) *S'il est vrai qu'il faut abattre des barrières, il en est aussi d'utiles et de nécessaires. Le jour où, au sein de l'État, chaque fonctionnaire qui détient une parcelle de la puissance publique pourrait tout savoir de chaque homme, de chaque famille, de chaque entreprise, ne voit-on pas à quels risques l'administré serait exposé ? »* [1]

Conséquence de cette autolimitation de l'efficacité administrative, les administrations ont fait porter aux usagers le poids d'une certaine complexité administrative. C'était à l'usager d'assurer la continuité du traitement de son dossier entre les différentes administrations, notamment en assurant lui-même la transmission des informations entre services. Cette exigence de protection de la vie privée est loin d'être la cause unique ou centrale de la complexité administrative. Il en est d'autres, à commencer par une culture administrative fondée sur la défiance, qui traite les usagers comme des fraudeurs en puissance, et conduit à exiger d'eux des monceaux de pièces et d'attestations pour justifier de leur situation.

1. *Rapport de la Commission informatique et libertés*, 1975.

L'irruption des technologies de l'information et de la communication, parce qu'elles facilitent considérablement des échanges d'informations jusqu'alors difficiles et coûteux à organiser, change la donne.

C'est donc ce pacte conclu dans les années soixante-dix que l'administration électronique nous conduit (et nous contraint) à réévaluer.

Le nouveau pacte, à renégocier, reposerait sur la confiance de l'administration à l'égard des usagers. L'administration électronique conduit à réviser certaines procédures : à réévaluer, par exemple, l'ensemble des pièces et documents que l'administration a pris l'habitude d'exiger. La réflexion en cours à la Commission des simplifications administratives (COSA) sur les concours administratifs débouche sur l'idée qu'il n'est pas nécessaire d'exiger une copie des diplômes de tous les candidats mais des seuls candidats admissibles ou des seuls candidats admis.

La confiance des usagers vis-à-vis de l'administration conditionne très largement l'essor de l'administration électronique. Elle dépend de la capacité des administrations à restituer aux usagers l'information qu'elle détient sur eux. Les formulaires (imprimés ou numériques) pré-remplis vont dans ce sens : l'usager peut vérifier la pertinence de ce qu'une administration sait sur lui. L'administration pourrait aussi, à partir de la connaissance qu'elle a des situations personnelles, informer les usagers sur les droits qu'ils peuvent exercer.

Pluralité des accès

Le défi principal que rencontre le développement de l'administration électronique sera d'éviter l'exclusion d'une partie de la population et, au-delà, l'apparition d'une administration à deux vitesses.

La Mission rappelle, à la suite du rapport Lasserre [1] qui appelait au développement d'une « administration à accès pluriel », que l'administration électronique ne saurait se limiter au tout-internet. Bien au contraire, quel que soit le média utilisé, l'administration électronique doit améliorer le service rendu à l'usager. La refonte des processus administratifs, rendue nécessaire par les téléservices, va en effet rendre possible une diversification des modes d'accès et de fourniture des services publics :
– par téléphone : ce qui suppose la mise en place de centres d'appels spécifiques à un ministère ou interministériels ;
– à partir de bornes interactives, consultables dans des lieux publics : mairies, administrations, etc. ;
– à partir de n'importe quel guichet.

Un usager devra pouvoir effectuer ses démarches à partir de n'importe quel guichet : dans sa mairie, dans les préfectures, dans les

1. Bruno Lasserre, *L'État et les technologies de l'information et de la communication*, Commissariat général du Plan, La Documentation française, 2000.

maisons des services publics, voire à partir du guichet de son administration la plus proche, sans dégradation ni surcoût. Cela suppose que les agents publics, dans ces guichets, disposent d'un terminal, aient reçu la formation nécessaire et aient le temps d'aider les usagers à effectuer leurs démarches en s'appuyant sur les systèmes d'information créés à cet effet.

L'administration électronique n'a pas pour objectif, et ne saurait avoir pour résultat, de permettre à l'administration d'augmenter le niveau de contrôle et de surveillance des citoyens

Le rapport Carcenac, après avoir décrit l'administration en réseau, soulignait que cette évolution *« doit se faire dans la transparence, en garantissant les libertés mais en profitant pleinement de la technologie. Cela nécessitera vraisemblablement une réflexion sur l'adaptation des textes réglementaires (loi informatique et liberté) aux évolutions technologiques, ainsi que l'ont initiée la Suède et le Royaume-Uni ».*

Cette adaptation réglementaire est en cours. Le projet de loi révisant la loi de 1978 afin de transposer la directive a été adopté (en première lecture) par l'Assemblée nationale.

Pour la Mission, le développement de l'administration électronique devrait pouvoir se faire dans le cadre législatif actualisé. Il ne requiert pas, au moins avant longtemps, d'assouplissement.

Au reste, l'administration électronique ne vise pas à recueillir des informations nouvelles sur les usagers. L'enjeu consiste, au contraire, à donner accès aux usagers aux données qui les concernent et qui existent aujourd'hui dans les systèmes d'information des administrations.

Être alerté quand une administration demande un extrait de casier judiciaire, être prévenu des contrôles effectués sur sa déclaration de revenus, avoir accès à l'état de son dossier, suivre à la trace son dossier de permis de construire au sein des administrations qui le traitent successivement : tous ces services n'accroissent en rien les connaissances que les administrations ont sur l'usager. Elles augmentent, en revanche, la connaissance qu'a l'usager de ce qui le concerne : elles améliorent son autonomie et sa capacité d'action.

Un grand nombre de téléservices s'effectuent et devront pouvoir s'effectuer de manière anonyme, sans contrôle d'accès ni identification

L'immense majorité des services en ligne proposés par les administrations sont accessibles aujourd'hui sans aucune forme d'identification. Des dispositifs d'identification devront être mis en place sur le ou les portails publics, dans la perspective du ou des « comptes administratifs personnalisés » en vue de sécuriser les échanges de données confidentielles ou d'effectuer des opérations (comme le télépaiement). L'existence de ces dispositifs n'implique cependant en aucune façon qu'on rende obligatoire l'identification préalable pour des services qui ne le nécessitent pas.

« Cela vaut pour les services de base mais aussi pour des services avancés ou personnalisés comme la simulation d'impôts, la fourniture régulière d'informations à partir d'un profil, l'adaptation d'un site en fonction de la localisation géographique ou du statut (ex. particulier/entreprise) d'un usager » [1]. L'utilisation d'un pseudonyme suffit largement pour assurer la personnalisation d'un service : ainsi, le site de prévention de la toxicomanie drogues.gouv.fr permet aux personnes de poser des questions extrêmement précises en utilisant un pseudonyme. Dans le cadre d'un portail, il devrait être possible de regrouper sous un seul pseudonyme les services proposés par plusieurs administrations, sans pour autant rendre obligatoire une identification plus avancée.

La maîtrise des données personnelles : un principe nécessaire mais à enrichir

Pour sauvegarder la vie privée, la loi informatique et liberté a consacré une double approche de la protection des données : d'une part, un encadrement « par le haut », avec des régimes d'autorisation par la CNIL pour la création de fichiers administratifs et, d'autre part des droits reconnus aux usagers pour un contrôle « par le bas », afin de vérifier la légalité des traitements et l'exactitude des données (droits d'accès, de communication, de rectification et d'opposition). Dans la pratique, c'est la première approche qui a principalement prévalu : les traitements de données sont rigoureusement examinés au stade de leur création, mais, et c'est peut-être un signe de confiance dans ce contrôle, l'exercice direct de leurs droits par les usagers est resté largement théorique. Les droits d'accès, de communi-

1. Jacques-François Marchandise, Fondation internet nouvelle génération.

cation et de rectification, qui ne peuvent s'exercer que par courrier, sont peu utilisés dans la pratique.

Avec le développement de l'administration en ligne, il est possible d'enrichir ces droits des administrés, pour qu'ils permettent une véritable maîtrise des données par les personnes. Une telle maîtrise signifie pour les usagers un véritable accès en ligne aux systèmes qui contiennent des données à leur sujet, non pour seulement pour en vérifier l'exactitude, mais aussi pour en obtenir la communication sous forme numérique. À titre d'exemple, si l'accès et la communication, tels qu'ils sont aujourd'hui conçus, aux fichiers des diplômés des universités ont pour seul objet d'en vérifier l'exactitude, un droit de communication permettrait à ce diplômé d'obtenir une copie numérique de son diplôme pour le joindre à son CV ou s'inscrire en ligne à un concours administratif.

Dans la même perspective, au lieu d'adresser une pièce justificative papier à une administration, on pourrait donner son consentement à ce que, pour une demande très déterminée, elle se fasse communiquer une information par une autre. Il ne s'agit là que d'une transposition à la société de l'information de la pratique de communication des pièces justificatives. Si l'objectif est donc d'ores et déjà perceptible, les modalités de sa mise en œuvre restent quant à elles à définir. Il s'agit que ce droit de disposition des données, qui implique par nature un consentement de la personne concernée puisqu'il est exercé par cette personne, ne résulte pas d'un consentement extorqué.

S'il s'agit d'une autorisation donnée à une administration pour qu'elle se fasse communiquer une information par une autre, il faut que cette autorisation soit précisément délimitée, révocable et exercée sous le contrôle d'une instance indépendante : la CNIL. Sans que toutes les réponses soient déjà dessinées, on conçoit que de nouveaux équilibres puissent se dessiner pour permettre une véritable maîtrise des personnes sur leurs données qui, sans atténuer les contrôles qui existent, leur reconnaisse de nouveaux droits.

Intérêt et limite des solutions dites de « coffre-fort électronique »

Un certain nombre de solutions technologiques permettent de placer les données personnelles sous le contrôle effectif des personnes. Elles constituent, en un sens, la traduction technique du principe de maîtrise des données personnelles. Ces solutions ont reçu le nom de « coffre-fort électronique ».

La métaphore du coffre-fort suggère que les données personnelles sont « enfermées » quelque part (sous clef) et que seule la personne concernée (son détenteur ou son « propriétaire ») est habilitée à y accéder pour transmettre ces données. Pour aller puiser ces données dans le

coffre-fort, les interlocuteurs (entreprises ou administrations) doivent obtenir son autorisation et, éventuellement, la clef.

Cette notion de coffre-fort renvoie à une grande diversité de dispositifs et d'architectures. Le coffre-fort peut ainsi être installé sur l'ordinateur de la personne, sous son contrôle direct, ou chez un intermédiaire public ou privé (un « notaire » ou « tiers de confiance » ou « infomédiaire »). Ce coffre-fort peut être lui-même compartimenté en zones : une clef spécifique donne alors accès à chacune de ces zones. En lieu et place d'une clef unique, l'utilisateur se voit doté d'un trousseau de clefs électroniques.

L'intérêt des outils et systèmes techniques qui renforcent la maîtrise des individus sur leurs données personnelles est indiscutable. Ils permettent d'exercer, de manière effective, les droits déjà consacrés par notre législation. Ils ne se substituent pas pour autant au cadre législatif protecteur de la vie privée. En tout état de cause, il revient à la CNIL de définir un cadre général permettant de protéger les usagers, notamment les plus fragiles ou les plus insouciants, contre eux-mêmes.

Quel que soit le degré d'implication et de délégation à des opérateurs tiers, l'État garde une fonction d'encadrement et de définition des règles

Pour la mise en place de l'administration électronique, l'État devra clarifier les diverses fonctions qu'il exerce :
– le pilotage et l'animation de l'administration électronique ;
– la production de services : ceux-ci reposent, pour une très large part, sur les systèmes d'information ;
– la distribution de services.

La clarification de ces trois fonctions est d'autant plus importante que l'administration électronique déborde largement le cadre des seuls services de l'État. Elle inclut les institutions de protection sociale et les collectivités territoriales. De surcroît, l'administration électronique présente une forte composante technologique et fait appel à des technologies développées par des opérateurs privés.

La fonction de pilotage sera essentielle

En s'assignant l'objectif de la généralisation des téléservices, le gouvernement indique clairement qu'on sort d'une logique ou chaque administration développe ses propres téléprocédures, à son rythme et en fonction de ses moyens et objectifs propres. La généralisation des téléser-

vices nécessite un pilotage politique, un pilotage opérationnel (le « chef d'orchestre » de Thierry Carcenac), ainsi que des structures spécialisées d'appui.

Le pilotage politique du chantier de l'administration électronique repose aujourd'hui sur les comités interministériels pour la réforme de l'État (CIRE). Présidés par le Premier ministre, préparés par le ministre de la Fonction publique et de la Réforme de l'État, les CIRE inscrivent l'administration électronique dans le cadre global de la modernisation de l'administration.

La mise en œuvre des décisions prises dans ces instances revient, cependant, largement aux ministères. L'informatisation est conduite aujourd'hui sous la responsabilité de chaque ministre, qui reste libre des orientations données au développement du système d'information de son ministère. Obligation lui est faite cependant de rédiger un schéma directeur informatique (SDI) sur une base pluriannuelle de trois à cinq ans.

La coordination des différents ministères est assurée par la constitution de groupes de travail et de réflexion, sous l'égide de la délégation interministérielle à la réforme de l'état (DIRE) sur les aspects fonctionnels et organisationnels de la modernisation des services [1].

À l'heure actuelle, plusieurs structures administratives différentes interviennent, chacune dans leur domaine de compétence :
– la délégation interministérielle à la réforme de l'État (DIRE) ;
– l'agence des technologies de l'information et de la communication dans l'administration (ATICA) [2] ;
– la commission pour les simplifications administratives (COSA) ;
– la direction centrale de la sécurité des systèmes d'information (DCSSI).

La question du pilotage opérationnel reste ouverte. Le rapport Carcenac avait esquissé un certain nombre d'options.

Production des services publics : les systèmes d'information

Pour assurer des services personnalisés, rendre possible l'accès des usagers à leur compte et à leur dossier, les administrations vont devoir opérer une refonte de leurs systèmes d'information. À défaut, et comme le soulignait Thierry Carcenac, les services que l'on peut offrir en ligne sont condamnés à plafonner. Pour prendre une analogie dans le secteur privé, la première étape de l'administration électronique peut se comparer à l'informatisation des agences de voyage, la deuxième étape correspond à la mise

1. Elle organise en particulier des réunions périodiques des hauts fonctionnaires de modernisation, représentants nommés par chaque département ministériel.
2. Techniquement, le pilote devra s'appuyer sur les standards techniques internationalement reconnus. Le cadre commun d'interopérabilité préparé par l'ATICA est une étape dans cette direction. L'administration gagnera à s'appuyer sur le développement de logiciels libres qui donnent une réalité technique opérationnelle aux standards ouverts.

en place du système SABRE de réservation électronique généralisée des voyages et des séjours.

Dans le passé, les administrations se sont souvent contentées de reformer l'interface (comme elles l'avaient fait à l'époque de la télématique). La refonte des systèmes d'information administratifs représente un effort considérable, compte tenu de leur complexité. Il faut investir dix fois plus pour réformer le système d'information que pour réformer l'interface. À titre d'exemple, la refonte du système d'information de la direction générale des impôts (Copernic) représente un budget de 90 millions d'euros par an. Ce projet mêle, ce qui est toujours souhaitable, l'objectif de réformer le service et celui de moderniser le système d'information.

Certaines administrations préféreront déléguer l'exploitation proprement informatique à des opérateurs. Qu'elles exploitent elles-mêmes ou qu'elles délèguent, les administrations devront néanmoins conserver la maîtrise des systèmes d'information sur lesquels reposent les services publics.

La distribution des services publics

L'administration électronique tend à unifier la distribution des services publics à travers des portails gouvernementaux, des guichets électroniques uniques, des centres d'appels, des maisons de service public dédiées à un type d'usagers et non à un type de prestations. Un très grand nombre de procédures présentent de surcroît un caractère triangulaire : elles font intervenir des institutions, publiques ou privées, dont les usagers sont clients ou affiliés (banques, associations, etc.). Les téléservices publics devront donc s'articuler (s'interfacer) avec un certain nombre de services assurés par des opérateurs privés.

Certaines fonctions de distribution pourraient par ailleurs être déléguées à des opérateurs privés. C'est le choix que font les pays anglo-saxons. Ces questions d'imbrication entre téléservices publics et téléservices privés se posent de manière aiguë pour tout ce qui tourne autour de la gestion des identités numériques et de l'authentification : coffre-fort électronique, certificat et signature électronique, infrastructures de gestion de clefs. Les opérateurs tiers privés (notamment ceux qui opèrent sur une base mondiale) auront donc tendance à proposer chacun leur solution technique (souvent propriétaire). Si l'administration tarde à définir une architecture ouverte et des règles du jeu, le risque n'est pas négligeable que ce soient les opérateurs privés qui dictent leurs solutions.

La sécurité des téléservices

La sécurité des systèmes informatiques sera un élément essentiel de la confiance des usagers et donc de leur adhésion à l'administration électronique.

La confiance désormais repose sur deux éléments :
– le sentiment que l'État prend les mesures de sécurisation nécessaire dans la manière dont il constitue et gère ses systèmes d'information (voir encadré) ;
– la possibilité que des experts issus de la société civile puissent s'en assurer par eux-mêmes. L'opacité des logiciels propriétaires s'oppose ici à ce type de contrôle. Cela plaide pour l'utilisation de logiciels au code source ouvert dans l'administration électronique.

Sécurité des systèmes, sécurité des échanges

• *La sécurité des systèmes consiste à protéger les ordinateurs et les données stockées contre les intrusions, les virus, les vols ou les dommages causés aux données. Le chiffrement des données, l'authentification des personnes en droit d'y accéder, font (éventuellement) partie de cette sécurité, mais d'autres éléments entrent en jeu : contrôle des accès au réseau et aux machines, vérification anti-virus, surveillance des usages, interdiction d'un certain nombre de fichiers ou de protocoles techniques, etc.*

• *La sécurité des échanges porte, d'une part sur les accès aux systèmes et aux données, d'autre part sur les échanges de messages et de documents via les réseaux. Compte tenu des données confidentielles qui s'échangent à travers les téléservices, l'architecture des téléservices et le « compte administratif personnalisé » devront garantir :*
– l'authenticité : prouver son identité à un interlocuteur, établir l'origine d'un message ;
– la confidentialité : transmettre un message et archiver des données, sur un réseau (ou un média) non sécurisé, de manière à ce qu'un tiers ne puisse pas en prendre connaissance ;
– l'intégrité des données : vérifier que des données n'ont pas été altérées lors d'un échange, ou dans le temps.

La cryptographie à clef publique semble devoir être la technique à partir de laquelle il est possible de traiter simultanément ou de manière séparée ces trois éléments.

Les choix français doivent être le plus harmonisés possible avec les choix européens

Tous les pays de l'Union ont mis en place des programmes, plus ou moins ambitieux. Les chefs d'État et de gouvernement ont adopté au Conseil européen de Santa Maria da Feira (juin 2000) un plan d'action « e-Europe 2002 ». Ce plan consacre un chapitre à l'administration électronique. Il assigne aux administrations publiques des États membres six séries d'objectifs, assortis d'un calendrier.

Les directeurs généraux en charge de la fonction publique des États membres de l'Union européenne se réunissent désormais régulièrement. Il s'agit principalement, à ce stade, d'examiner des sujets d'intérêt commun (la présidence suédoise a retenu le thème de l'identification électronique) et d'examiner les réalisations avancées (les *« best practices »*). Il faudrait aller bien au-delà de l'échange de vue : une véritable concertation se révélera rapidement nécessaire entre administrations européennes.

Cette concertation n'ira pas de soi. Soucieux d'accompagner un champion industriel national ou, plus prosaïquement, de partager les investissements avec des industriels, certains gouvernements européens commencent en effet à nouer des partenariats avec les acteurs industriels.

Au premier rang des questions qui pourraient donner lieu à concertation figure celle des techniques d'identification, de la signature électronique, des infrastructures de clef publiques, des futurs supports d'identité (carte d'identité électronique), de l'interopérabilité, de la conduite à tenir vis-à-vis d'offres techniques proposées par des acteurs déjà prépondérants. On pourrait imaginer que les administrations européennes engagent un dialogue avec la *Liberty Alliance* pour définir, avec les industriels, les standards ouverts de l'identification et de la protection des données personnelles en ligne.

Troisième partie

Questions pour le débat

Chapitre 1

Statut des données personnelles

Les personnes sont-elles propriétaires des données qui les concernent ?

Alors que la loi dote les individus de droits d'accès, de communication, de rectification et d'opposition sur leurs données qui restent relativement théoriques, la réalité de la société de l'information voit proliférer les collectes et les ventes de données à des fins marchandes, au point que le principal droit sur les données semble parfois être un droit de propriété. Si une telle analyse patrimoniale devait prévaloir, les traitements administratifs et leur régime de contrôle pourraient en subir les effets.

Cela justifierait en effet une approche contractuelle de la maîtrise des personnes sur leurs données, et cela remettrait en question le contrôle opéré sur les traitements administratifs, qui est protecteur mais aussi contraignant pour les usagers comme pour les administrations. C'est pourquoi il faut se demander comment doivent s'analyser juridiquement les droits des usagers sur leurs données.

Il est tentant en première approche de regarder les personnes comme détentrices d'un véritable droit de propriété sur leurs données.

• C'est la perception intuitive, qui veut que selon des modèles économiques du web naguère très florissants, mais toujours présents, on cède ou « vende » ses données personnelles, en échange notamment de services gratuits. Et il est vrai que si un droit de propriété doit être reconnu sur les données personnelles, ce droit de propriété devra plutôt être conféré à la personne qui est concernée par les données qu'au détenteur de la base de données. Il s'agit là d'une exception au principe suivant lequel l'information appartient à celui qui en réalise la collecte ou qui en assure la formulation. En effet, les données personnelles que des administrations peuvent détenir sur les usagers (nom, date de naissance, domicile, situation familiale, voire revenu imposable ou contenu du casier judiciaire) sont des données objectives, que les administrations se bornent à relever sans y ajouter une appréciation subjective qui justifierait une appropriation de leur part. S'il y a un droit de propriété sur les données personnelles, ce ne peut donc être que celui de la personne qui est concernée.

• De sérieux arguments conduisent à récuser cette idée d'un droit de propriété sur les données personnelles. Ces données personnelles, qui reposent sur un fondement objectif, ne peuvent pas être modifiées à loisir par la personne concernée, sauf naturellement si la modification de la donnée correspond à une modification dans la situation objective correspondante (domicile, nom, etc.).

• Pour un véritable droit de propriété, il manque donc un élément de libre disposition du bien. Au stade de leur formulation, ces données ne sont pas davantage l'œuvre de l'intéressé que de l'administration : cette formulation *« dépend de la loi (dévolution du nom, détermination de l'état civil, du domicile, etc.), ou bien elle s'attache de plein droit aux actes du sujet (acquisitions immobilières, état des comptes bancaires, condamnations pénales, etc.) »* [1].

• Au surplus, l'idée d'un droit de propriété n'est pas celle qui fonde la législation sur l'informatique et les libertés, bien davantage centrée sur une optique de protection des libertés. Or, pour reprendre une formulation américaine à propos de ce même débat sur les données personnelles, *« un droit de propriété peut être vendu mais les droits de l'homme ne peuvent jamais faire l'objet de transactions »* [2].

• Soustraire ainsi les données personnelles au champ du droit de propriété est une position de principe et peut se rapprocher des dispositions existantes en matière d'interdiction de commercialisation des éléments du corps humain. Cela ne frappe sans doute pas d'interdit les pratiques consistant à rémunérer le temps passé par les personnes à communiquer les informations qui intéressent les gestionnaires de bases de données. Mais cela interdit que la communication d'une donnée puisse être regardée comme la cession d'un droit patrimonial sur celle-ci.

• Enfin, s'agissant spécifiquement des données détenues par l'administration, l'usager peut se trouver contraint de consentir à la communication de données. En application de l'article 26 de la loi du 6 janvier 1978, le citoyen peut se voir privé de l'exercice de son droit d'opposition à ce que des données le concernant figurent dans un traitement public. De même, la directive communautaire du 24 octobre 1995, si elle consacre en son article 7 le principe du consentement de la personne comme une des conditions légitimant le traitement de données, prévoit également que le traitement est légitime s'il est nécessaire au *« respect d'une obligation légale à laquelle le responsable du traitement est soumis »* ou encore à *« l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique »*.

Ainsi la cession à l'administration d'une donnée personnelle n'est-elle pas purement discrétionnaire et ne saurait elle s'analyser dans une optique contractuelle. Elle peut s'imposer comme une exigence de la collectivité pour rendre possible la vie en commun, dans une logique proche de celle qui fonde l'impôt [3].

1. P. Catala, « Ébauche d'une théorie juridique de l'information », repris *in Le droit à l'épreuve du numérique,* « Jus ex machina », PUF, 1998.
2. Margaret-Jane Radin, professeur de droit à Stanford, cité par Arnaud Belleil, *ePrivacy*, Dunod, 2001.

Au total, l'analyse la plus rigoureuse semble donc conduire à analyser les données personnelles non en termes de droit patrimonial mais en termes d'attributs de la personnalité : *« bien que la personne concernée ne soit pas "auteur" de l'information, au sens de la mise en forme, elle est le titulaire légitime de ses éléments. Leur lien avec l'individu est trop étroit pour qu'il puisse en être autrement. Quand l'objet des données est un sujet de droit, l'information est un attribut de la personnalité »* [1]. Ce caractère d'attribut de la personnalité signifie que la communication des informations doit résulter soit du consentement de l'intéressé, soit d'obligations législatives ou réglementaires.

Au-delà du débat doctrinal, tout l'enjeu de la législation est alors d'assurer les conditions de la maîtrise des personnes sur ces données, en leur reconnaissant un véritable droit à déterminer l'usage qui doit être fait des données personnelles détenues par les administrations. C'est la mise en œuvre de la théorie de l'autodétermination informationnelle, par laquelle le tribunal constitutionnel fédéral allemand [2] a proclamé le droit pour l'individu de décider de la communication et de l'emploi des informations relatives à sa personne.

Quelles limites au principe de maîtrise des données ?

Le principe de maîtrise des données personnelles ne saurait être posé en absolu. Il s'exercerait dans cette zone de latitude, dans ces cas et ces situations, où la décision de communiquer ou non certaines données personnelles, d'autoriser leur transmission d'une administration à une autre, peut avantageusement être laissée à l'initiative des personnes. Dans cette zone de latitude, c'est à la personne de décider, en fonction des avantages qu'elle attend ou des risques qu'elle redoute, de communiquer ou non ses données, d'autoriser ou non l'administration qui détient les données qui la concernent à les transmettre à une autre administration.

Ainsi, les formulaires (pour les procédures qui s'y prêtent) pourraient distinguer les questions qu'il faut remplir impérativement de celles qui sont facultatives. Un justiciable qui demande l'aide juridictionnelle pourrait autoriser la direction générale des impôts à transmettre l'avis de non-imposition nécessaire pour en bénéficier. Cette zone où s'exerce l'initiative de communiquer ou non des données personnelles, d'autoriser ou non la transmission de données entre deux administrations, en tout état de cause, serait doublement bornée :

3. Cf. la notion d'« impôt informationnel » développée par J-M. Bruguière, *La diffusion de l'information publique : le service public face au marché de l'information*, thèse de doctorat soutenue le 23 juin 1995, université de Montpellier I.

1. *Ibid.*

2. Tribunal constitutionnel fédéral allemand, jugement du 15 décembre 1983 relatif au recensement de la population.

– d'un côté, par le caractère obligatoire de certains recueils de données personnelles. Le principe de maîtrise des données personnelles ne saurait faire obstacle à l'accomplissement d'objectifs d'intérêt public ou qui présentent un caractère obligatoire : certaines procédures, formulaires ou recueils d'information par l'État présentent un caractère obligatoire [1] ;
– de l'autre, par des règles qu'il reviendrait à la CNIL d'édicter, afin de protéger les personnes, notamment les plus vulnérables, contre la curiosité des administrations (« protéger les personnes contre elles-mêmes »).

Faut-il bâtir l'administration électronique sur la base des systèmes d'information traditionnels, ou en déplaçant le centre de gravité des données personnelles vers l'usager ?

Sans doute convient-il de distinguer ici deux approches pour les systèmes d'information de l'administration.

• Dans la première approche, traditionnelle, l'administration continue de conserver et de gérer les données sur les usagers. Le changement réside dans la fluidité qu'autorise la refonte des systèmes d'information.

Dès lors que l'usager peut accéder en ligne à son compte ou à son dossier, il peut exercer de manière effective les droits d'accès et de rectification. On peut, dans ce cadre traditionnel, envisager une extension des droits existants. Des systèmes d'information administratifs performants permettraient de passer d'un droit d'information préalable à un droit d'information « permanent » : chaque fois qu'une donnée (ou un ensemble de données) fait l'objet d'une modification, ou d'une transmission à une autre administration, elle peut aisément notifier ces changements à la personne.

En termes techniques, on pourrait imaginer que *« la personne, publique ou privée, qui a besoin d'une information concernant une autre personne dont elle pense qu'elle est déjà détenue par une administration compétente devra en priorité avoir recours à la consultation de cette information et n'exiger la duplication de l'information requise que lorsque celle-ci est nécessaire dans l'exécution d'un traitement ou lorsque la valeur prise par cette donnée est susceptible d'être modifiée, de façon à préserver cette valeur pour la procédure à l'origine de la requête. »* [2]

• Dans la seconde approche, c'est un changement radical qui s'opère. On bascule vers un système d'information *distribué*. Les données

1. 2e alinéa de l'article 26 de la loi de 1978.
2. Louise Cadoux et Annie Marcheix, contribution au forum de discussion du rapport *Pour une administration électronique citoyenne*, mai 2001.

personnelles sont placées sous le contrôle effectif de l'usager. Quand l'administration en a besoin, elle les demande : l'usager les lui transmet ou autorise l'administration à aller les chercher là où elles se trouvent.

Pour illustrer la nature de changement, on pourrait prendre l'exemple de l'automobile. Le constructeur ne détient que très peu de données sur l'automobile et son propriétaire. Les données relatives au fonctionnement de l'automobile sont conservées dans l'électronique de l'automobile. Si l'automobiliste rencontre un problème, il « autorise » le système de diagnostic électronique à transmettre les données au constructeur. Dans une architecture distribuée, la question du droit d'accès et du droit de rectification ne se pose pas pour les données qui sont sous le contrôle direct de l'usager.

Ces deux approches ne sont pas incompatibles. L'une des clefs du succès de l'administration électronique réside dans la combinaison entre l'approche classique et l'approche distribuée. Une voie de développement de l'administration électronique consisterait à utiliser dans un premier temps l'approche classique, plus facile à mettre en place, puis à basculer progressivement vers l'approche distribuée, qui assure à l'usager une maîtrise plus complète de ses données personnelles.

Recentrage des systèmes d'information administratifs et individualisation

Pour s'engager dans les téléservices, donner accès au compte et au dossier personnel, les administrations vont devoir engager une refonte de leurs systèmes d'information autour des personnes. C'est un processus lourd, qu'ont amorcé il y a vingt ans les banques et les grands opérateurs de réseaux (France Télécom, EDF) pour que leurs clients puissent consulter leurs comptes et effectuer des opérations en ligne.

Les controverses passées et récentes autour des identifiants ont accrédité le sentiment que les systèmes d'information administratifs fichaient les personnes de manière systématique. La réalité est plus nuancée. Si les systèmes d'information administratifs recueillent de nombreuses informations sur les personnes, ils sont, le plus souvent, organisés autour d'une procédure. Ainsi, de nombreux systèmes d'information gèrent des actions ou des programmes : ils recensent, bien sûr, les bénéficiaires (les personnes, par exemple, qui ont suivi les actions de formation) et les données associées à ces personnes, mais ils ne sont pas nécessairement conçus pour reconstituer le profil de chaque personne (reconstituer, par exemple, l'ensemble des formations suivies par une personne). Orientés vers la production d'indicateurs (combien de gens bénéficient de telle ou telle prestation ?), ils se soucient peu du profil individuel des bénéficiaires.

Les systèmes d'information de l'administration fiscale, emblématiques d'une informatique inquisitrice, ne procèdent que très indirectement à un fichage des personnes. Ils sont constitués d'une série d'applications, organisées chacune autour d'un impôt : impôt sur le revenu, taxe d'habitation, taxe foncière. Chaque application a des identifiants distincts, qui ne reflètent pas la même identité : foyer fiscal, indivision, bien immobilier. C'est tout l'enjeu du projet Copernic que de refondre les systèmes d'information autour de la personne. Cette refonte ouvrira la voie au compte fiscal simplifié, mais aussi à une individualisation de la fiscalité ; l'individualisation de l'impôt sur le revenu est déjà pratiquée dans les pays qui ont instauré le prélèvement de l'impôt à la source.

Indice de cette individualisation : un couple pourrait avoir le choix entre imposition commune ou imposition séparée. Dans l'imposition séparée, chaque conjoint déclare son propre revenu et son propre patrimoine. La notion de « vie privée » se déplace : la confidentialité se glisse à l'intérieur même du couple ou du foyer. Une personne pourrait déclarer à l'administration fiscale des biens ou des revenus alors que son conjoint pourrait en ignorer l'existence. Sous cet angle, le recentrage des systèmes d'information autour de la personne va bien au-delà d'une simple rationalisation. Elle accompagne et radicalise les tendances socioculturelles qui placent l'individu au centre du fonctionnement de nos sociétés. C'est une question qui se posera pour l'instauration du compte administratif personnalisé : sera-t-il centré sur la personne ou sur le foyer ?

Chapitre 2

Architecture de l'administration électronique

Code informatique, code juridique

Les principes de protection de la vie privée sont aujourd'hui définis par le législateur et deviennent opérationnels grâce à l'action de la CNIL. Mais dans la mesure où il s'agit d'informatique, le logiciel peut faciliter ou empêcher les atteintes à la vie privée. On peut ainsi se demander si le code informatique peut se substituer au code juridique.

Le juriste américain Lawrence Lessig a montré que les principes de liberté et de coopération qui sont au cœur d'internet sont incorporés dans les logiciels de base du réseau des réseaux. Dans la même perspective, on peut imaginer que les règles de protection des données personnelles soient inscrites dans les logiciels eux-mêmes. Dans cette nouvelle approche, le législateur continuerait à fixer les grands principes mais le travail réglementaire serait profondément allégé, puisque les règles de protection de la vie privée seraient directement incorporées dans les logiciels. Le citoyen aurait ainsi une garantie beaucoup plus forte sur le fait que sa vie privée serait effectivement protégée. Un tel choix ne modifie pas seulement les modes de production du droit, mais aussi ceux des programmes informatiques. Pour s'assurer que les logiciels intègrent bien les règles de protection des données personnelles, il est indispensable que les logiciels de base ne soient pas propriétaires, qu'il s'agisse de programmes ouverts auxquels tout informaticien peut donc accéder. Dans cette perspective, la CNIL devrait être chargée d'une mission de contrôle des grandes caractéristiques des logiciels, afin d'examiner si les informaticiens ont bien transformé le droit en code informatique.

On l'aura compris, cette nouvelle approche qui peut être particulièrement efficace pour assurer une protection maximum de la vie privée amène à modifier profondément les modes de production du droit et des logiciels informatiques. La Mission estime donc qu'il y a là une question importante à soumettre au débat public.

Un compte unique ou plusieurs « comptes thématiques » ?

L'un des fils conducteurs de l'administration électronique consiste à « unifier » l'accès aux services de l'État, et plus généralement aux services publics. Une première étape est accomplie : le portail www.service-public.fr. La seconde étape est celle de la mise en place d'un « point d'entrée » donnant accès, sous la forme d'un « compte », personnalisable, à l'ensemble des téléservices, à travers un système de contrôle d'accès (identification). Trois solutions sont envisageables.

La mise en place d'un guichet unique : le « compte administratif personnalisé »

Cette solution offre le grand avantage de permettre à l'usager d'accéder de façon unifiée, et donc aisée, à l'ensemble des services publics en ligne qui le concernent.

« Compte citoyen », « compte administratif », « guichet en ligne », « guichet unique », « portail personnalisé ». La désignation de ce « point d'entrée unique » reste hésitante. C'est néanmoins bien le type d'architecture que mettent en place les administrations irlandaise avec *Public Services Broker*, britannique avec *Government Gateway*, suédoise avec *Government E-Link*. C'est également la perspective qu'a dessinée le comité interministériel pour la réforme de l'État de novembre 2001 avec le projet *mon.service-public.fr*.

Plusieurs portails thématiques

Cette solution correspond à l'évolution tendancielle des administrations. Un certain regroupement de l'offre de téléservices est d'ores et déjà en train de s'opérer autour d'un petit nombre de pôles ou sphères administratives :

– le ministère de l'Économie, des Finances et de l'Industrie met en place un portail fiscal qui donnera accès au compte fiscal ;

– dans la sphère de la protection sociale, Net-Entreprises unifie, pour les entreprises, l'ensemble des télédéclarations sociales des entreprises (à terme, Net-Entreprises pourrait proposer des services aux salariés). L'assurance maladie a ouvert un service téléphonique, AlloSécu : la version internet d'AlloSécu constitue l'amorce d'un compte de l'assuré social ;

– la sphère éducative, autour du ministère de l'Éducation. Le projet I-prof est aujourd'hui destiné aux personnels enseignants. Chaque enseignant peut, au travers d'I-prof, consulter son dossier administratif, le compléter, consulter des guides thématiques, dialoguer avec son correspondant de gestion pour lui signaler un changement dans sa situation personnelle ou administrative, lui poser une question... Le ministère de l'Éducation pourrait, à terme, mettre en place un service comparable pour les usagers : élèves et parents.

Toutes ces initiatives tirent parti de l'existence d'un identifiant qui permet d'effectuer le contrôle d'accès pour l'accès au compte : NIR pour la sphère sociale, numéro fiscal pour la sphère sociale, Numen pour la sphère éducative. Cette approche multi-portails, chaque portail utilisant un identifiant spécifique semble convenir à la CNIL, légitimement hostile à la mise en place d'un identifiant unique, soucieuse de cantonner les identifiants existants aux sphères concernées.

La faiblesse de ce scénario, c'est qu'il laisse de côté les ministères et les institutions qui n'ont pas la capacité, ou la masse critique, pour composer une offre conjointe autour de portails sectoriels. Cette collection de portails sectoriels serait également *a priori* moins simple d'utilisation pour l'usager qu'un portail unique.

Grappes de services transversales à plusieurs ministères et services publics

Cette approche « par la demande » se veut transversale par rapport à la précédente, qui est plutôt orientée « par l'offre », puisque les téléservices ne sont pas organisés par secteur institutionnel mais par type de besoin concret des usagers. Chacun des téléservices qui mettent en jeu plusieurs administrations (ce que les Canadiens appellent « grappes de services ») requiert alors la mise en place d'un dispositif spécifique.

On pourrait se satisfaire, dans un premier temps, d'une approche pragmatique qui consiste à identifier les téléservices prioritaires, comme la télédéclaration de changement d'adresse. Le gouvernement québécois envisage ainsi de développer des grappes de services pour les étapes qui rythment la vie des citoyens : naissance, mariage, emploi, changement d'adresse, décès.

Quel type de « compte administratif personnalisé » ?

On peut, à la suite de Daniel Kaplan (FING), envisager trois scénarios.

• **Scénario du « coffre-fort à distance »** : les usagers acceptent de confier à l'administration, sur un site web « portail » des téléservices, des données personnelles incluant éventuellement des données d'identification. Les usagers peuvent aussi demander sur ce site à récupérer auprès des administrations des données les concernant, qui sont alors stockées au sein du « coffre-fort » avec celles qu'ils ont eux-mêmes fournies. Ainsi, l'usager peut croiser certaines données, faciliter le « passage » de données d'un « silo » administratif vers l'autre, etc. – mais dans une zone neutre et inaccessible aux autres administrations. Le site permet enfin

de transmettre en une fois certaines données à plusieurs administrations (exemple : changement d'adresse).

• **Scénario du « coffre-fort à domicile »** : le compte administratif personnalisé est avant tout une zone de stockage de données personnelles placée sous le contrôle direct de l'utilisateur (sur son ordinateur, dans un dispositif portable comme une carte à puce, etc.). Il permet notamment à un usager de stocker des données personnelles, des certificats et d'envoyer à diverses administrations des requêtes et des ordres standardisés. Il ne se substitue pas aux sites web des différentes administrations dans la relation avec les usagers, mais il est interopérable avec les systèmes d'information des différentes administrations. La structure des données et des messages est standardisée. D'un point de vue technique, il gère également un annuaire, un système de vérification d'identités, de droits, de certificats et un système de routage de requêtes aux administrations.

• **Scénario de la « maison de service public virtuelle »** : il s'agit d'un service auquel l'usager donne, ponctuellement ou de manière plus durable, des mandats précis : collecter et lui livrer certaines informations (personnelles et non personnelles), réaliser des transactions (exemple : changement d'adresse), exécuter des ordres. Le modèle est en quelque sorte celui d'une maison de service public – les services publics de proximité utilisant le même système d'information que la maison de service public virtuelle. Certains mandats peuvent être exécutés de manière totalement automatique. Le service peut également intervenir comme un « masque » : il est habilité à demander certaines informations à certaines administrations de la part d'un usager, dont l'administration n'a pas nécessairement à connaître l'identité. Certaines procédures peuvent impliquer, à un certain moment, le retour vers un interlocuteur, par courrier électronique ou par téléphone. Le traitement des dossiers peut y gagner en transparence et en rapidité. L'usager serait alors orienté vers un interlocuteur polyvalent. Celui-ci assurerait pour l'essentiel une fonction de pilotage au sein de l'administration. Il devrait disposer des outils techniques pour s'assurer du suivi, de la « traçabilité » des demandes au sein de l'administration. Il assurerait l'interface entre l'usager et les agents en charge du traitement des demandes.

Quelles modalités d'identification et d'accès à ce compte administratif ?

Dans les scénarios qui précédent, on constate que le regroupement de services ne signifie pas nécessairement le regroupement et le croisement de données par l'administration elle-même. En réalité, les scénarios qui précèdent se croisent avec des scénarios concernant l'organisation des clefs d'identification.

• **Scénario « clef unique »** : une clef d'identification maîtresse et bien sécurisée ouvre l'accès à un dispositif de stockage de la plupart des informations sensibles de l'usager. C'est le scénario britannique. Pour s'inscrire puis accéder à *Government Gateway*, il est nécessaire de disposer au préalable d'un certificat numérique personnel. Ce certificat doit être référencé dans la liste des certificats reconnus digne de confiance par les services du *Government Gateway*. Pour l'usager, c'est le scénario le plus simple.

• **Scénario « clefs multiples »** : l'usager dispose d'un outil qui lui permet d'utiliser plusieurs clefs pour accéder, éventuellement de manière simultanée, à plusieurs téléservices. Il peut y avoir besoin d'une clef pour « ouvrir » le porte-clefs, mais il n'y a pas ensuite de hiérarchie entre les clefs : l'utilisation de chaque clef exige de suivre les procédures d'identification *ad hoc*. Ce scénario intègre au niveau technique la nécessité de séparer de manière absolue des données relevant de « sphères » administratives distinctes : santé, fiscalité, emploi, éducation, etc. Pour l'usager, c'est le scénario le plus protecteur.

• **Scénario mixte** : une clef générique permet d'accéder à un dispositif de stockage regroupant à la fois certaines données personnelles peu sensibles, accessibles directement, et d'autres données plus sensibles – ces dernières étant elles-mêmes protégées par des clefs multiples au sens du scénario précédent.

Signature électronique et infrastructures à clefs publiques : une solution publique ou une panoplie de solutions ?

Les banques fournissent depuis des années des services en ligne dont l'accès est protégé par un simple couple identifiant – mot de passe. Dès lors, on peut légitimement s'interroger sur la nécessité de subordonner le développement de téléservices publics à l'utilisation d'outils de type « signature électronique », au moins pour les années à venir. La plupart des démarches administratives ne sont pas, en effet, dans leur version traditionnelle, lourdement sécurisées, ce qui est un gage de leur ergonomie.

S'il s'avère néanmoins que l'accomplissement de certains téléservices exige l'utilisation de la signature électronique, notamment pour des raisons juridiques ou à la demande de la CNIL, alors cette authentification devra bénéficier de toutes les garanties techniques et organisationnelles en matière de sécurité et de protection des données personnelles.

L'utilisation de la signature dans le cadre de l'administration électronique soulève, au moins, trois types de questions :

– la reconnaissance par les téléservices publics des signatures électroniques « privées » (délivrées par les opérateurs privés : les « tiers de confiance »). C'est par exemple l'option retenue par le ministère de l'Économie, des Finances et de l'Industrie pour TéléTVA ;
– la mutualisation : les outils de signature électronique mis en place ou reconnus dans le cadre d'une démarche gérée par une administration devraient pouvoir être reconnus par une autre administration ;
– la mise en place d'une forme de « service public » de la signature électronique. Le ministère de l'Économie, des Finances et de l'Industrie – pour les impôts des particuliers – et Net-Entreprises – pour les professionnels – envisagent également de distribuer eux-mêmes et gratuitement, au moins dans un premier temps, de tels certificats. C'est également l'option retenue par le gouvernement canadien [1].

Ces options ne sont d'ailleurs pas exclusives. La meilleure solution serait sans doute de pouvoir proposer aux usagers de l'administration une panoplie de solutions de sécurité. Certaines de ces solutions seraient publiques, afin de fournir un service universel, mais d'autres pourraient être privées (banques, etc.). Cela n'est pas sans poser des questions en terme d'ergonomie et de facilité d'emploi.

Faut-il un support physique pour gérer les clefs et les signatures ?

Les questions qui précédent se croisent avec une autre famille de questions : faut-il privilégier une solution technique pour le stockage et la gestion des clefs et signatures ? La carte à puce, les clefs USB, les supports sans contact, le téléphone portable figurent parmi les nombreuses options pour fournir le support de cette sécurité. Le candidat le plus sérieux semble être la carte à puce : l'usage de la carte bancaire a familiarisé des millions de Français avec cet outil.

L'utilisation de la carte à puce suppose l'existence d'un lecteur. Ce peut être un frein : pour utiliser la carte à puce, les usagers devraient disposer, à leur domicile ou dans tout autre endroit ou ils souhaitent procéder à des téléservices, d'un lecteur. Les fabricants d'ordinateur (majoritairement américains) ne prévoient pas d'intégrer de lecteur de cartes dans la prochaine génération d'ordinateurs de bureau ou d'ordinateurs portables. La promotion de l'administration électronique (et plus généralement des services en ligne qui requièrent de la confiance) interfère ici avec des considérations de politique industrielle. Le GIE Carte bancaire

1. En revanche, il ne semble pas que les responsables de SESAME-Vitale souhaitent doter la carte d'assuré social d'une telle fonctionnalité, alors que la carte de professionnel de santé (CPS) permet la signature électronique. S'agissant d'un domaine très sensible, il semble effectivement réaliste de ne pas utiliser SESAME-Vitale ou la carte CPS dans d'autres « sphères » administratives que la santé.

envisage d'intégrer des certificats électroniques dans la Carte bleue. L'évolution des lecteurs de carte à puce d'un appareil à usage financier vers un outil de « sécurisation universel » est à l'ordre du jour et donne lieu à des projets industriels (comme le projet européen Finread).

Les solutions matérielles (cartes à puce, téléphone portable, clef USB, *token*, etc.) facilitent l'appropriation par le public et comportent un élément de confiance. Les solutions logicielles semblent cependant nettement plus faciles à déployer, puis à maintenir, puisqu'il n'y a pas de flux physiques ; c'est tout particulièrement vrai par rapport à des solutions imposant non seulement la gestion d'objets d'identification, mais également de périphériques informatiques (lecteurs).

Les solutions reposant sur des mesures biométriques (empreintes digitales, iris, reconnaissance faciale, forme de la main, etc.) cumulent les avantages des solutions immatérielles (absence de déploiement) et matérielles (on possède au sens physique la clef d'accès). Une forte incertitude technique et financière sur leur déploiement à grande échelle fait néanmoins douter de leur utilisation à court terme. Elles sont de surcroît, traditionnellement, liées aux techniques de surveillance et de répression de la criminalité et apparaissent donc excessives au regard des finalités de l'administration électronique courante.

Là encore, la meilleure solution serait sans doute de pouvoir proposer aux usagers de l'administration une panoplie de solutions.

Une carte d'identité dotée d'une puce électronique pourrait-elle devenir l'outil d'accès aux téléservices publics ?

Dès lors que la version électronique de la carte nationale d'identité disposerait d'une puce, elle pourrait être dotée d'une fonction de signature électronique : celle-ci pourrait alors être utilisée pour donner accès à des téléservices en ligne pour lesquels serait exigée l'authentification. Cette fonctionnalité pourrait être utile dans certaines fonctions spécifiques à la gestion de l'identité par le ministère de l'Intérieur (changement d'adresse, renouvellement de carte, par exemple). Elle pourrait également servir, au-delà, de système d'authentification générique pour l'accès et l'utilisation des téléservices publics. En d'autres termes, une carte nationale d'identité électronique pourrait être un candidat à la fourniture d'un « service public » de la signature électronique. C'est l'objectif de la carte d'identité électronique mise en place en Italie ou en Finlande.

Mais l'intégration de la signature électronique ne risque-t-elle pas d'inquiéter les usagers en associant sur un même support physique deux fonctionnalités *a priori* très différentes : le contrôle de l'identité (qui

reste la fonction première de la carte d'identité) et l'accès aux services de l'administration électronique ?

En tout état de cause, la carte d'identité n'est pas accessible aux étrangers, qui pourtant doivent pouvoir bénéficier d'une égalité d'accès aux services de l'administration. Si était mise en place une carte d'identité électronique intégrant la fonction de signature, il conviendrait donc de prévoir une carte électronique dotée d'une fonction équivalente de signature pour les étrangers.

Chapitre 3

Droits, services, fonctionnalités

Comment l'usager délègue-t-il aux administrations le droit d'utiliser ses données ?

Le regroupement de services ne signifie pas nécessairement le regroupement et le croisement de données par l'administration elle-même. La mise en œuvre des téléservices transversaux n'exige pas nécessairement l'interconnexion des systèmes d'information des administrations concernées. Dès lors qu'un certain nombre de données personnelles sont placées sous le contrôle direct de l'usager, les interactions avec les téléservices reposent sur un principe d'autorisation. L'usager donne son accord pour communiquer des données à l'administration concernée (ou, ce qui revient au même, pour qu'elle aille les chercher, là où elles sont stockées). L'autorisation peut être soumise à des conditions :
– autorisation ou non d'inscription de ces données dans le système d'information ;
– durée de conservation ;
– non-transmission à une autre administration.

En fonction de la nature des données, ces autorisations d'utilisation des données personnelles pourraient être permanentes (mais révocables), renouvelées régulièrement (pour une période), données au cas par cas.

Peut-on rendre opérationnel le principe selon lequel tout accès ou modification des données personnelles qui concernent un usager dans les bases de données publiques devrait donner lieu à une notification ?

La refonte des systèmes d'information permet de rendre effectif le droit d'information. *« Le citoyen doit avoir une visibilité entière sur la gestion par les administrations de l'information le concernant. Qui a consulté quoi, quand et pour quels motifs ? Qui a dupliqué quoi, quand et pour quel usage ? Qui a modifié une information, à quelle date, pour quelles raisons et quelles en sont les conséquences au sein de l'administration compétente et au sein des administrations utilisatrices ?* » [1]

L'administration aurait l'obligation d'informer le citoyen de ces modifications. On peut imaginer que cette obligation de notification ne revêt pas la même forme selon le degré de sensibilité des données en cause, ou encore selon le « cycle de vie » des données : certaines données sont fréquemment modifiées alors que d'autres dorment dans les systèmes d'information. On peut envisager, une obligation de notification à chaque modification. Cette notification peut aussi être mensuelle ou annuelle. Elle revêtirait alors le caractère d'un « bilan informationnel ». Cette notification permettrait d'exercer le droit de rectification, si l'usager constatait que la modification a entraîné une erreur.

Un « bilan des droits » régulier pourrait-il être organisé ?

Jacques Attali, dans un article récent [2], posait cette question : *« combien de citoyens ne connaissent pas leurs droits, ne savent pas quelles aides leurs sont dues ?* (...) *L'administration le sait si bien qu'elle évalue le coût budgétaire d'une mesure sociale en espérant qu'un quart ou plus des bénéficiaires ne se manifesteront pas. Et ce sont évidemment toujours les plus démunis qui en pâtissent le plus. Connaître ses droits est un privilège de plus en plus chèrement acquis. »*

Il suggérait que l'État informe chaque citoyen individuellement de ses droits, comme il l'informe des impôts ou des cotisations dont il est redevable. *« Comme on demande chaque année au citoyen de remplir une*

1. Louise Cadoux et Annie Marcheix, contribution au forum de débat du rapport *Pour une administration électronique citoyenne*, mai 2001.
2. Jacques Attali, « Devoir d'État », *L'Express*, novembre 2001.

déclaration d'impôt, il pourrait remplir, s'il le voulait, une "déclaration de droits", permettant à l'administration de déterminer les prestations et les exonérations auxquelles le citoyen a droit et s'obligeant à les lui faire connaître. Les nouvelles technologies peuvent rendre cela plus facile encore : chacun aura bientôt la possibilité de remplir sa déclaration d'impôt par l'internet et pourra recevoir ainsi prestations et informations. Réciproquement, l'internet permettrait aisément à l'État de fournir en temps réel, individuellement, à chaque citoyen, dans des conditions de grande confidentialité, toutes les informations sur ce qui lui est dû. »

De nombreux citoyens ignorent les prestations et les aides auxquelles ils ont droit. D'ores et déjà, le portail Service-public.fr permet de trouver l'ensemble de ses droits et démarches. Il est d'ailleurs utilisé par les personnes en difficulté et par les intermédiaires sociaux, comme en témoigne la liste des mots le plus souvent recherchés sur son moteur de recherche : SMIC et RMI font partie des dix mots les plus recherchés.

Jacques Attali, par symétrie avec la déclaration annuelle des revenus, envisageait une « déclaration des droits » annuelle. *A priori*, toujours sous réserve d'une refonte des systèmes d'information de l'administration, on peut imaginer que le compte administratif personnalisé fournira, non pas une fois par an, mais pratiquement chaque fois que l'usager le souhaite (à chaque connexion), un « bilan des droits ». Ce check-up des droits pourrait figurer, à terme, parmi les services proposés par le « compte administratif personnalisé ».

La réalisation d'un tel bilan suppose, il est vrai, la compilation d'un grand nombre d'informations, issues de diverses bases de données administratives. Il serait effectué de telle manière que seule la personne concernée puisse y accéder.

On peut se demander si un outil de simulation (sur le modèle de la simulation d'impôts, avec un niveau de complexité supérieur) ne remplirait pas le même service. À l'initiative directe de l'usager, celui-ci pourrait, comme il peut le faire dans les simulations fiscales, modifier des paramètres pour « optimiser » l'accès à certaines prestations.

Secteur public, secteur privé : qui fournit les services d'administration électronique ?

L'administration électronique a de nombreux points communs avec les services marchands en ligne. Elle est organisée selon un principe de séparation entre le contact avec le public (*front office*) et le traitement de l'information (*back office*), elle utilise des systèmes informatiques qui ont beaucoup de similitude avec ceux des banques ou des compagnies d'assurances. Les grandes sociétés d'informatique (Microsoft, HP, IBM, etc.) utilisent des outils voisins pour la mise en ligne des services

marchands ou non-marchands. Enfin, les entreprises et l'administration collaborent parfois dans certains domaines. Ainsi, le fichier des véhicules automobiles est-il géré conjointement par les constructeurs automobiles et par l'administration.

Dès lors qu'il y a une telle proximité entre l'administration électronique et les services marchands en ligne, certaines téléprocédures administratives pourraient sans doute être distribuées par des entreprises privées telles que les banques, les compagnies d'assurances, ou les mutuelles. L'usager aurait ainsi le choix de son distributeur, la compétition entre les entreprises concernées permettrait sans doute d'augmenter l'efficacité et de faire baisser les coûts. Cette ouverture au privé est-elle souhaitable ? Des entreprises privées peuvent-elles assurer l'égalité de tous devant le service public ? Moyennant quel système de régulation ? Comment se rémunéreraient-elles ? Cela implique-t-il que certaines téléprocédures soient payantes ? Que l'État rémunère des intermédiaires qui rendraient des services plus efficacement que lui ?

Quoi qu'il en soit, cette hypothèse n'est pas purement spéculative. La diffusion des services en ligne pourrait amener à modifier les frontières entre le public et le privé. Il est utile d'ouvrir le débat sur cette question et de comparer les solutions publiques et privées en termes d'efficacité, de qualité et d'universalité des services.

Chapitre 4

Pilotage et mise en œuvre

Mise en œuvre : comment déployer l'administration électronique ?

Le gouvernement s'est assigné un objectif de généralisation des téléservices. Le premier aspect de la généralisation concerne le déploiement des téléservices au sein de l'administration. On sort d'une logique d'expérimentation où chaque administration développe ses propres téléprocédures, à son rythme, en fonction de ses priorités et des moyens (humains, budgétaires, techniques) dont elle dispose. La logique d'expérimentation, nécessaire dans un premier temps, débouche sur des disparités. Certains ministères ont des programmes ambitieux (le ministère de l'Économie, des Finances et de l'Industrie consacre des moyens considérables à sa mutation en e-ministère) alors que d'autres, comme le ministère de la Justice, vont nettement moins vite.

La généralisation peut se faire en concentrant les moyens sur un certain nombre de téléservices prioritaires (prioritaires au regard des attentes des usagers, en volume d'opérations), puis, à partir de ces réalisations, étendre les téléservices à l'ensemble des administrations. Elle peut aussi se faire en déployant, de manière volontaire, un certain nombre de services et de ressources mutualisés : un réseau (il existe : Ader), un portail (il existe : Service-public.fr), les maisons des services publics (elles se mettent en place, mais, sans accès direct aux systèmes d'information des administrations, ce qui limite leur portée), un dispositif d'accès au compte administratif personnalisé (c'est là que se portent les interrogations : voir plus haut les scénarios), éventuellement, une infrastructure de clef publique, un serveur de télépaiement, un ou des centres d'appels.

Par ailleurs, l'État devra se coordonner avec les différentes collectivités territoriales de façon à unifier et rapprocher l'administration du citoyen.

Comment favoriser l'utilisation des téléservices par les usagers ?

Au regard des moyens mobilisés, il n'est pas indifférent que les téléservices rencontrent lentement ou très vite l'adhésion du public. Pour favoriser l'usage des téléservices, les administrations pourraient mettre en œuvre des incitations. L'usage des téléservices pourrait donner lieu à un allégement des exigences et des formalités.

Incitation

L'article 6 de la loi de finances pour 2002 a prévu un allégement procédural pour ceux qui transmettent leur déclaration de revenus par voie électronique. À la différence de ceux qui transmettent leur déclaration de revenus par voie postale, ceux qui la transmettent par voie électronique ne sont pas tenus de joindre le justificatif de la réduction qu'ils demandent au titre des cotisations syndicales versées. Le principe de tels allégements ne va pas de soi, au regard du principe d'égalité. Dans ce cas précis, le Conseil constitutionnel a jugé que *« la disposition critiquée a pour simple objet de favoriser la déclaration de revenus par voie électronique ; elle ne dispense pas de la production de ces pièces lors d'un contrôle fiscal ultérieur ; ainsi, elle n'est pas contraire au principe d'égalité »* [1].

L'usage des téléservices pourrait aussi donner lieu à une incitation financière : une réduction de l'imposition (pour la télédéclaration de revenus), par exemple. Par l'instauration d'une incitation financière, l'administration concernée restituerait, en somme, au contribuable une partie des gains de productivité générés par la numérisation de la procédure. C'est un raisonnement du même ordre qui conduit les caisses d'assurance maladie à reverser une somme fixe au médecin pour chaque feuille de soin télétransmise. On peut également s'inspirer de l'exemple italien : l'administration fiscale reverse une somme fixe pour chaque déclaration fiscale télétransmise. Les syndicats ont mis en place un service d'assistance pour aider les salariés à télédéclarer leurs revenus en ligne, et reçoivent de l'administration fiscale une somme fixe pour chaque télédéclaration.

Substitution

Au-delà des incitations, il y a aussi la substitution pure et simple de la téléprocédure à la procédure traditionnelle. Ce qui revient à rendre obligatoire la téléprocédure. C'est l'option qui a été retenue par la direction des impôts pour la télédéclaration de la TVA (TéléTVA). Toutes les entreprises ayant un chiffre d'affaires de 100 millions de francs (17 400 entreprises concernées) sont désormais tenues de déclarer la TVA par voie électronique. Mentionnons également le cas d'une téléprocédure assez

1. Décision du Conseil constitutionnel du 27 décembre 2001 à propos de l'article 6 de la loi de finances pour 2002.

ancienne, RAVEL (Recensement automatisé des vœux des élèves) qui n'existe que sous forme de téléprocédure (sur minitel ou sur internet). RAVEL permet aux nouveaux bacheliers de s'inscrire dans les universités en formulant des choix. Un principe de sectorisation permet, en cas de déséquilibre entre les demandes et les capacités d'accueil des universités, d'affecter les candidats dans l'université la plus proche de leur établissement d'origine. La sectorisation est établie grâce à un logiciel de calcul des temps de transport, et à partir des vœux des lycéens.

Envisager une telle approche pour les particuliers se heurte, là aussi, au principe d'égalité. En tout état de cause, ceux-ci devraient pouvoir faire appel à l'aide d'agents publics spécialisés ou de médiateurs associatifs ou commerciaux.

Conclusion

À l'issue de ce périple, qui nous a conduit du parapheur à la signature électronique, de l'univers du guichet à celui des technologies de pointe, qu'il nous soit permis de livrer une réflexion qui déborde le cadre de la mission qui nous a été confiée.

Dans un environnement technologique évolutif, la tentation est forte d'attendre que les forces du marché sélectionnent (et, au final, imposent) des solutions technologiques. L'autre écueil, c'est le choix d'une solution technologique, voire industrielle, qui se révélerait par la suite isolée par rapport aux acteurs économiques et aux autres administrations européennes.

C'est bien entendu au gouvernement que reviendra, à l'issue du débat public, de définir une stratégie pour l'administration électronique qui tire tout le parti, dans un contexte technologique incertain, des solutions disponibles mais également ouverte à celles qui apparaîtront dans les années à venir.

Contributions extérieures

Interconnexions, NIR [1] et téléprocédures : position actuelle de la CNIL [2]

Contribution de la CNIL

Rappel des principes de protection des données personnelles

Le principe de finalité

Un traitement ne peut être mis en œuvre que pour une finalité déterminée, explicite et légitime correspondant aux missions de l'organisme, tout détournement de finalité étant passible de sanctions pénales.

Pas d'utilisation des fichiers administratifs à des fins politiques ou commerciales.

Le principe de pertinence et de proportionnalité des données

Les données doivent être adéquates, pertinentes et non excessives par rapport à la finalité du traitement.

Restrictions à l'enregistrement des informations faisant apparaître les origines raciales ou les opinions politiques, philosophiques ou religieuses ou les appartenances syndicales ou les mœurs des personnes, les infractions, condamnations ou mesures de sûreté.

Le principe d'une durée de conservation limitée des informations sur support informatique

Les informations ne doivent être conservées que le temps nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées. Au delà, elles ne peuvent être conservées, après tri opéré en accord avec l'administration des archives, qu'à des fins historiques, statistiques ou scientifiques.

1. NIR : Numéro d'Inscription au Registre national d'identification des personnes physiques (RNIPP).
2. CNIL : Commission nationale informatique et liberté.

L'obligation de ne communiquer les données qu'aux destinataires et aux tiers autorisés à en connaître

Les données nominatives ne peuvent être communiquées qu'aux destinataires et aux tiers autorisés à en connaître en vertu de la loi.

Distinction entre la notion de destinataires, autorisés à recevoir régulièrement communication d'informations, et la notion de tiers autorisés habilités à obtenir, de façon ponctuelle et motivée, des informations détenues dans des fichiers (autorités judiciaires agissant dans le cadre de commissions rogatoires, services fiscaux dans le cadre du droit de communication).

L'obligation de sécurité

Toute personne ordonnant ou effectuant un traitement d'informations nominatives doit prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés.

Le respect des droits des personnes : principe de loyauté et de transparence

Droit d'être informé des conditions d'utilisation de ses données et en particulier des transmissions envisagées.

Droit de s'opposer, sous certaines conditions, au traitement de ses données.

Droit d'accès à ses informations, de les faire rectifier voire supprimer.

Les interconnexions

Le principe de finalité justifie les précautions prises en matière d'interconnexions qui, constituant un nouveau traitement, sont à ce titre, soumises à l'avis de la CNIL. Le projet de loi modifiant la loi de 1978 maintient un régime de formalités pour les interconnexions.

Nécessité d'un fondement légal aux interconnexions de fichiers

Lorsqu'elle est saisie d'une interconnexion de fichiers, la CNIL s'assure qu'elle peut légalement avoir lieu. Ainsi, dans le domaine social, les rapprochements de fichiers, parce qu'ils concernent des

informations couvertes par le secret, **résultent tous de dispositions législatives spécifiques précisant les finalités de ces rapprochements**.

Principe de « finalité » de l'interconnexion

Les interconnexions ont généralement pour but **de vérifier la réalité de la situation administrative ou socio-économique des usagers**. **La Commission n'a jamais contesté la légitimité de cet objectif de contrôle mais a estimé nécessaire de recommander, en contrepartie, de réelles simplifications des démarches administratives. Ainsi a-t-elle approuvé les échanges d'informations instaurés, depuis 1995, entre la CNAVTS [1] et la DGI [2], pour obtenir directement de cette direction les avis de non imposition.**

L'obligation d'information des personnes

Les personnes concernées doivent être clairement informées du sort des données collectées et des organismes destinataires.

L'obligation de sécurité

Les dispositions prises pour assurer la confidentialité des informations sont examinées avec attention, en particulier lorsque les informations sont transmises par réseau (chiffrement).

Le NIR

La loi de 1978 puise ses origines dans la crainte que l'informatisation de l'administration et les interconnexions entre fichiers publics ne portent atteinte à la liberté des citoyens. C'est d'ailleurs un projet d'interconnexion généralisée, sur la base du NIR, de tous les fichiers administratifs, dévoilé dans les années 70 sous le nom de « SAFARI », qui a abouti au vote de la loi.

Le NIR, un numéro pas comme les autres

En raison de ses origines, de sa composition et de son caractère signifiant : créé sous le régime de Vichy, le NIR est associé à une symbolique du « repérage » des individus. Reflet, sous forme numérique, de l'identité de chacun, le NIR est, de fait, plus aisé à utiliser dans les applications informatiques. Dès lors, la tentation est toujours grande, plutôt que de désigner les individus par leur état civil complet, de faire appel de

1. CNAVTS : Caisse nationale d'assurance vieillesse des travailleurs salariés.
2. DGI : direction générale des Impôts.

préférence à des numéros qui facilitent ainsi l'accès aux fichiers et les interconnexions.

Le recours au NIR est donc aujourd'hui strictement encadré par la loi et par la CNIL (autorisation par décret en Conseil d'État pris après avis de la commission).

État de la doctrine de la CNIL sur l'utilisation du NIR : pragmatisme et vigilance

Pragmatique : plus d'une cinquantaine de décrets autorisant l'utilisation du NIR ont été adoptés après avis de la CNIL dans le domaine social (organismes de sécurité sociale, employeurs, ASSEDIC, ANPE, organismes d'assurance maladie complémentaires, professionnels de santé...).

Vigilante et soucieuse de cantonner le NIR à la « sphère sociale », la Commission a dès l'origine entrepris de convaincre les administrations de se doter d'un numéro spécifique. Ainsi, le ministère de l'éducation nationale a finalement, en 1992, substitué le NUMEN au NIR, comme identifiant principal, dans ses fichiers de gestion des personnels.

Une utilisation encadrée du NIR dans la sphère fiscale

L'article 107 de la loi de finances pour 1999 autorise désormais les administrations financières à utiliser les NIR des contribuables dans leurs traitements, ainsi que pour la communication, aux organismes de sécurité sociale et de retraite complémentaire, des informations nécessaires à l'appréciation des conditions d'ouverture et de maintien des droits aux prestations, au calcul de celles-ci, à l'appréciation des conditions d'assujettissement aux cotisations et contributions, à la détermination de celles-ci et à leur recouvrement.

En outre, cet article prévoit que lorsqu'est exercé le droit de communication auprès des organismes autorisés à utiliser le NIR, les informations nominatives communiquées mentionnent le NIR. Dans le cas où la mise en œuvre du droit de communication s'avérerait susceptible de porter une atteinte grave et immédiate aux droits et libertés, la CNIL peut enjoindre l'autorité administrative de prendre sans délai les mesures de sécurité pouvant aller jusqu'à la destruction des supports d'informations constitués à partir d'un NIR.

L'examen par la CNIL des décrets d'application lui a permis d'encadrer les conditions d'utilisation du NIR par les administrations fiscales, les modalités de conservation de ce numéro, le transfert sur la base du NIR de données fiscales aux organismes de protection sociale, ainsi que la liste des organismes habilités à communiquer le NIR aux administrations fiscales.

Ainsi, le NIR n'est présent et géré que dans des bases nationales (« table de correspondance NIR/n (SPI ») **et le numéro SPI continue à être utilisé comme identifiant fiscal personnel.**

Les conditions d'utilisation du NIR dans les interconnexions

Si l'interconnexion est autorisée par la loi, le NIR peut être utilisé, mais l'interconnexion ne doit pas être un vecteur de transmission du NIR à une administration qui n'aurait pas été préalablement autorisée à l'utiliser.

La Commission s'est ainsi prononcée favorablement en 1995 sur l'utilisation du NIR dans le cadre d'échanges entre les CAF et les ASSEDIC aux fins de vérification des droits des bénéficiaires du RMI et en particulier des ressources déclarées par ces derniers.

La CNIL a également émis un avis favorable en 2001 sur une procédure unique de transfert de données fiscales avec les organismes sociaux tous déjà autorisés à recourir au NIR.

Les téléprocédures

Les téléservices, dès lors qu'ils permettent de simplifier les démarches administratives et de rapprocher le citoyen de son administration, ne peuvent que rencontrer la faveur de la CNIL.

Depuis 1997, la CNIL s'est prononcée sur un certain nombre de télédéclarations, qu'il s'agisse des télédéclarations sociales par les entreprises, de la télétransmission des feuilles de soins, des télédéclarations de revenus, du télérèglement ou encore de la télédéclaration de TVA. La CNIL a également été consultée sur la demande par internet de certains extraits du casier judiciaire. De nombreuses collectivités locales l'ont saisie sur la mise en ligne de certains services (inscription scolaire, délivrance de fiches d'état civil, prise de rendez-vous avec les services municipaux...).

Lors de l'examen de ces projets, la CNIL **apprécie les dispositifs prévus pour garantir la confidentialité et l'intégrité des informations ainsi que l'authentification des usagers, en fonction en particulier du degré de sensibilité des informations, évoluant dans ses préconisations au fur et à mesure de l'évolution de la législation tant en matière de cryptologie que de reconnaissance de la signature électronique.**

Ainsi, la consultation en ligne du dossier administratif s'effectue généralement selon les dispositifs d'identification spécifiques aux systèmes d'information de chaque service public concerné.

S'agissant des télédéclarations, la CNIL a adopté le même raisonnement, à l'exception de la télédéclaration de revenus, pour laquelle elle a recommandé un identifiant spécifique plutôt que le n°de foyer fiscal, numéro non confidentiel car porté notamment sur les avis d'imposition, susceptible d'être communiqué à des tiers (organismes sociaux, bailleurs,...).

L'authentification s'effectue généralement par confrontation des informations communiquées par l'intéressé et des données détenues par l'organisme dans ses fichiers.

La reconnaissance juridique de la signature électronique reposant sur des infrastructures à clé publique s'est traduite, dans les avis rendus par la CNIL depuis 2000 sur les telédéclarations fiscales, par des recommandations fortes sur ce point. La CNIL s'était déjà prononcée favorablement en 1998 sur l'utilisation de la carte du professionnel de santé, pour signer, de façon électronique, les feuilles de soins télétransmises aux caisses de sécurité sociale.

Mais le recours systématique à ces procédés ne constitue pas aujourd'hui, pour la CNIL, une condition préalable à la mise en place des téléprocédures.

Tant que le droit, la technique et l'économie des infrastructures à clé publique ne seront pas totalement stabilisés, il serait en effet prématuré d'imposer des solutions qui méritent d'être évaluées en fonction de la finalité du téléservice public et du degré de sécurité que l'on en exige.

Le recours à des moyens de chiffrement pour assurer la confidentialité constitue un impératif dès lors qu'il s'agit de transmettre par internet des informations sensibles telles que des données de santé (recommandation du 4 février 1997).

Dans le domaine social, **La Commission a dès 1995, lors de l'avis rendu sur la mise en place du codage des actes de biologie télétransmis aux caisses de sécurité sociale par les professionnels de santé, considéré que les données d'identification des assurés devaient être chiffrées. À l'occasion de la généralisation du dispositif SESAME VITALE elle a, à nouveau, appelé l'attention des pouvoirs publics sur cette exigence.**

Des solutions de chiffrement ont également été prévues pour les télédéclarations sociales et fiscales. **La CNIL a ainsi estimé lors de l'avis rendu sur la procédure téléTVA que de tels dispositifs devaient être instaurés dès lors que la téléprocédure revêtait un caractère obligatoire.**

Les enseignements d'autres administrations européennes et du secteur privé dans le domaine des services en ligne

Contribution de l'ATICA
Jean-Pierre Dardayrol,
Juliette Campos Oriola
www.atica.pm.gouv.fr

Les expériences d'autres administrations européennes

Il existe aujourd'hui *une préoccupation commune* à la plupart des gouvernements européens quant à la mise en place de services en ligne pour les citoyens et les entreprises : passer de services verticaux, spécialisés par métier et étanches, à des systèmes horizontaux, ouverts, capables de communiquer entre eux et avec l'extérieur

Les différents états membres de l'Union Européenne qui prévoient la mise en œuvre de ces services dans le cadre des projets d'e-gouvernement convergent sur la cible et l'évolution des architectures fonctionnelles ainsi que sur le calendrier prévisionnel de mise en œuvre des services.

Les principales étapes envisagées sont dans l'ordre chronologique :
– l'information : sites informant l'usager sur les compétences, les attributions des administrations et proposant des données d'intérêt général ;
– l'interaction : services interactifs proposés sur des sites dynamiques avec des « formulaires intelligents », des moteurs de recherche évolués, des forums, des échanges par méls, etc,...
– les transactions : un site portail propose au public de déclencher en ligne, via un formulaire électronique, un processus de traitement ;
– enfin, la transformation : le service offert au public intègre complètement les services électroniques à son mode de fonctionnement et d'organisation, comme un moyen de gérer une approche orientée vers le citoyen, l'entreprise ou l'association.

Cette évolution devrait aboutir d'ici 2005 ; elle s'accompagnera d'une re-définition des services rendus, des processus, d'un changement d'organisation du travail et aboutira, *in fine*, à une approche centrée sur l'usager.

Il convient de souligner avec force que le développement de services en ligne à partir de procédures administratives complexes nécessite, à partir de la phase de transactions, d'importantes évolutions du *back-office* dans les domaines informatiques, informationnels, organisationnels et managériaux.

Ces évolutions mobiliseront des moyens humains, organisationnels, financiers, voire juridiques, importants ; elles nécessiteront du temps et une permanence dans la direction des administrations ; c'est ce que l'on appelle « *l'alignement stratégique* ».

En ce qui concerne ***l'architecture technique***, l'accord se fait sur un modèle intégrant l'ensemble des éléments matériels, logiciels et organisationnels nécessaires pour constituer une architecture complète de gouvernement électronique, depuis les infrastructures de transport des données jusqu'aux différents modes d'accès possibles pour les usagers.

Le modèle de référence est celui de la gestion de la relation client – GRC – qualifiée en anglais de CRM *(customer relationship management)* dans les applications dite « B to C » *(business to customer*).

Les objectifs annoncés des projets d'e-gouvernement sont les suivants : coopération fédérative, interopérabilité, échanges de données interapplicatifs, simplification des procédures, accès personnalisé des citoyens et des entreprises à travers des guichets d'accueil communs... jusqu'à un système d'information unitaire, en Italie par exemple.

Pour atteindre ces objectifs, *la mise en réseau des ressources physiques ou logiques et le partage des informations* entre les organismes sont nécessaires – en incluant ou non, selon les cadres institutionnels propres à chaque pays, les collectivités territoriales ou les organismes sociaux.

Dans certain pays – le Royaume-Uni, l'Irlande, la Suisse par exemple –, une articulation s'établit entre services du secteur public et ceux du secteur privé, notamment à travers des offres « franchisées » proposées par plusieurs prestataires selon un cadre défini par l'administration ; il s'agit par exemple de l'accès aux services publics à travers un portail internet généraliste. Est-ce alors simplement un canal ou lui délègue-t-on certaines fonctions : identification, paiement, archivage ?....

Au Portugal, le groupement cartes bancaires fournit des services d'e-administration à partir des distributeurs bancaires.

Les méthodes de mise en œuvre **sont proches :**
– la mise en place d'infrastructures et de services communs ;
– l'affichage de normes, référentiels et standards pour les systèmes d'information publics ;
– progressivement, la publication de schémas de données communs – mais beaucoup de répertoires de schémas XML restent vides.

Par contre *les stratégies* sont différentes :
– mise en œuvre ou non d'un cadre d'interopérabilité, plus ou moins obligatoire ;
– accompagné ou non de la mise en place d'éléments de *middleware* matériels et logiciels.

Les points critiques **sont en règle générale les suivants :**
– l'identification des personnes physiques et lien avec l'état civil ;
– l'authentification et les technologies associées (cartes, IGC...) ;
– la simplification des procédures consistant souvent dans un premier temps à masquer la complexité derrière l'automatisation des transferts de données ;
– les dictionnaires de données, souvent inexistants, difficultés pour unifier les définitions ;
– la nécessaire diversité des moyens d'accès ;
– les priorités et les attentes sociales.

Enfin il faut noter *l'importance du contexte***, notamment :**
– le taux d'accès internet ;
– le degré de centralisation et d'autonomie dans les choix des agences gouvernementales ;
– le rôle des collectivités territoriales et des organismes de « solidarité » ;
– l'importance du secteur public ;
– la sensibilité à l'utilisation des différents numéros d'identification (signifiants ou non, unique ou non...) ;
– la culture de « notarisation », plus importante au Sud qu'au Nord.

L'expérience du secteur privé : la GRC

Il s'agit d'un sujet d'investissement majeur pour les entreprises, même si les résultats en termes de services et de rentabilité ne sont pas encore à la hauteur des ambitions affichées.

Les entreprises en sont à différents stades d'intégration avec un objectif majeur : fidéliser en offrant le meilleur service grâce à une meilleure connaissance des clients.

Les initiatives viennent souvent du président dans une émulation entre les entreprises. L'urbanisation du SI apparaît comme un préalable, mais il est long et coûteux. On peut proposer de ce point de vue une typologie des entreprises :
– celles qui partent de zéro ;
– celles qui reconstruisent leur SI comme moteur de changement et d'adaptation, notamment à la suite de fusions – acquisitions ;
– celles qui disposent d'un patrimoine applicatif important et où la mise en place de la GRC a un fort impact sur le *back-office*.

Des exemples d'offre du marché

Certains gouvernements choisissent des sociétés comme conseils dans la mise en œuvre des projets d'e-gouvernement ; par exemple, HP en Suède. Le rôle de Microsoft est fort en Grande-Bretagne, celui d'IBM aux États-Unis.

L'offre *e-Governement* de HP est une offre globale pour une architecture complète d'e-gouvernment (annuaire des services, standards de communication...), avec des « pages jaunes » constituant l'annuaire des services en ligne et des accès multiples. Elle s'est développée à partir du programme suédois Government e-link.

Autre exemple : l'offre Passport de Microsoft qui propose une authentification fédérée et externalisée.

Les principaux enseignements

Il s'agit d'un engagement commun aux secteurs public et privé.

Face à la demande, on trouve une offre plurielle avec un ensemble de composants à différents niveaux de maturité et des garanties de pérennité inégales. La stratégie de mise en œuvre des projets requiert des efforts d'ouverture ou de conformité aux standards, une forme d'urbanisation du SI, la définition d'une politique d'identification et souvent un pilotage adaptatif.

Le portail de service public peut être conçu comme un simple facteur de simplification de la vie de l'usager ou comme un facteur de fédération beaucoup plus fort.

Des questions restent en suspens : l'intermédiation, l'archivage, etc.

Une approche des IGC et de leur organisation dans l'administration et les établissements publics

Contribution du SGDN

Introduction

Le secrétariat général de la défense nationale (SGDN), en liaison avec l'agence des technologies de l'information et de la communication dans l'administration (ATICA), anime depuis septembre 1999 un groupe de travail interministériel sur les infrastructures de gestion de clés (IGC) de répondre en particulier à ces questions :
– comment sécuriser les systèmes d'information fragilisés par de nombreuses et nouvelles interdépendances ?
– comment se préparer à l'interopérabilité que le concept d'IGC favorise ?
– comment mutualiser au sein de l'administration les expériences et les moyens ?

À partir de ces travaux et des orientations retenues par le cabinet du Premier ministre, il est proposé des mesures organisant les IGC de l'administration et des établissements publics, s'adaptant aux évolutions technologiques. Elles se sont concrétisées par l'offre de prestations nouvelles, *sur une base volontaire*, par la direction centrale de la sécurité des systèmes d'information (DCSSI) du SGDN.

Ces prestations sont présentés ci-dessous, après un bref exposé des motifs (§1) : enregistrement des IGC (§2), validation des accords de reconnaissance de certificats d'IGC (§3), et mise en place d'une autorité nationale de certification (§4).

Qu'est-ce qu'une IGC ?

Le rôle d'une IGC est de gérer des clés cryptographiques au profit d'une communauté d'utilisateurs qui les utilisent pour sécuriser des applications (messagerie électronique, *e*-commerce). Elle sert avant tout à distribuer des éléments d'information qui contribuent à l'authentification d'utilisateurs ou de machines (les certificats de clés publiques en particulier).

Le fonctionnement de l'IGC est régi par une politique de certification (PC) qui précise les objectifs de sécurité à atteindre, les devoirs, obligations et responsabilités envers les utilisateurs.

Une IGC se décompose en plusieurs composantes techniques :

• Les *autorités d'enregistrement* (AE) collectent les informations nécessaires à l'identification des utilisateurs et vérifient leurs droits.

• Les *autorités de certification* (AC) ont pour fonction de signer les certificats (qui sont principalement composés d'une clé publique et d'un identifiant d'utilisateur). Elles assurent la révocation des certificats qui ne sont plus de confiance.

• Le *centre de publication* (noté CP) assure la publication des certificats et des listes de révocation pour les applications utilisatrices et les utilisateurs finaux.

Pourquoi enregistrer les IGC ?

« La mise en place des téléprocédures de nouvelle génération nécessitera, pour chacune d'elle, des procédures d'authentification, de signature, de non-répudiation. Il faut dès à présent mettre en place une politique de certification interopérable entre les différents services de l'État. Elle devra être utilisable par tous, flexible en permettant d'avoir les renseignements nécessaires sur différents supports (disque dur, disquette, carte à puce) suivant les besoins et ouverte aux acteurs économiques de la certification qui respectent les normes. Il faut éviter le développement de différentes architectures incompatibles entre elles : cela pénaliserait le succès des téléprocédures. »

Rapport Carcenac – Proposition n° 30

Concernant les téléprocédures, M. Carcenac propose de créer une politique de certification partagée et compatible pour l'ensemble des administrations. Mais les métiers de la justice, de la santé, de la comptabilité publique, de la défense, de la diplomatie, de l'éducation et de la recherche ont leurs propres objectifs de sécurité et doivent définir en conséquence leur politique de certification. L'unicité d'une politique de certification pour l'ensemble des IGC semble difficile à atteindre compte tenu du large spectre des besoins fonctionnels et de la multiplicité des niveaux de sécurité visés.

Dès 1998, la commission interministérielle pour la sécurité des systèmes d'information (CISSI) a entrepris la définition d'une politique de certification (PC^2), véritable pivot autour duquel les politiques de certification des administrations se construisent. Elle est donc à la fois une aide à la rédaction et une référence commune. Il est préconisé que les administrations éditent leurs propres politiques de certification de façon harmonieuse au sein de chaque ministère.

La démarche repose sur la création de registres d'IGC, un par ministère et un registre interministériel au SGDN. Ces registres sont les

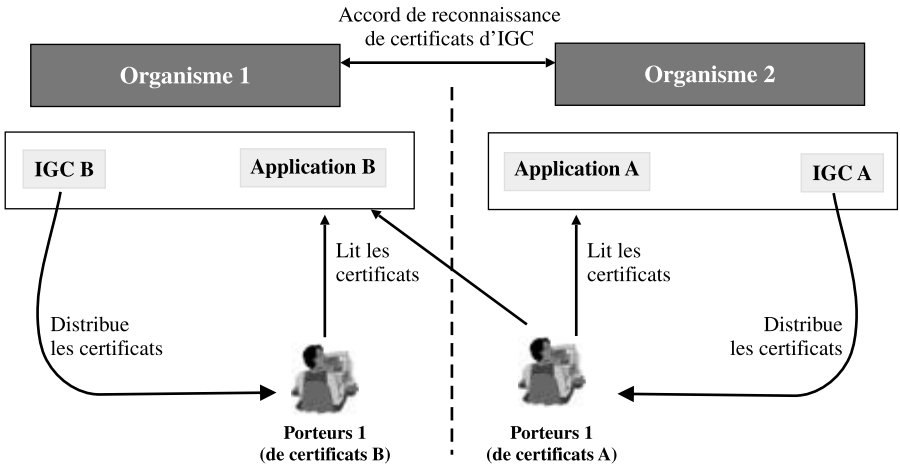
instruments permettant de construire des IGC autour de références, de parler un langage commun, de partager les expériences et le savoir, et de faire connaître plus facilement aux porteurs de certificats les éventuelles exigences que leur utilisation implique.

Pourquoi valider les accords entre ministères ?

M. Carcenac préconise d'éviter le développement d'architectures incompatibles entre elles. Or ce souci vaut pour tous types d'IGC : il faut s'attendre à ce que, pour des raisons d'économie et de rationalisation, les ministères ne voudront pas, d'une part multiplier les familles de certificats, ni d'autre part refaire un lourd travail d'enregistrement pour des agents d'autres ministères. C'est ainsi que naturellement se dessineront des accords bilatéraux pour s'en dispenser et simplement pouvoir reconnaître et lire des certificats d'IGC gérés par d'autres.

Apparaissent à ce stade les enjeux de sécurité. Chaque ministère maîtrise, sous sa responsabilité, la sécurité de ses systèmes d'information. Dès lors que se mettent en place des accords entre ministères, il s'avère nécessaire de mener un important travail technique de comparaison qui puisse être validé par un tiers, afin de vérifier la cohérence des choix de sécurité et leur bonne application dans la durée.

Cela se traduit de la façon suivante : un *accord de reconnaissance de certificats d'IGC* est pris entre deux organismes. Son objectif est de permettre à une population d'utilisateurs de certificats (Porteurs) émis par un Organisme 1 d'accéder de façon sécurisée à une Application sous la responsabilité d'un Organisme 2 et vice versa (cf. schéma ci-dessous).



Pourquoi une AC racine nationale ?

« ... À cet effet, et parce que certains ministères parmi les moins importants en taille ont tout à gagner de la mise à disposition d'une infrastructure à clef publique opérée pour leur compte par un opérateur public, il semblerait utile qu'une entité interministérielle propose – ou achète pour le compte de l'ensemble de l'administration – un service de gestion d'infrastructure à clef publique à un niveau de sécurité banalisé pour les agents publics. L'utilisation de cette infrastructure ne serait pas obligatoire, ce qui garantit qu'elle ne bloquerait pas le développement d'autres solutions mieux adaptées à certains projets ; elle aurait en revanche l'intérêt de faciliter le » décollage « de l'usage des IGC au sein de l'ensemble de l'administration. »

Rapport Carcenac – Proposition nº 31

Il est proposé aux ministères un service de certification interministérielle (noté IGC/A) d'autorités de certification. Ce service ne répond que partiellement à la proposition de M. Carcenac, car il ne s'agit pas pour la DCSSI de certifier des utilisateurs mais bien d'identifier les autorités de certification de plus haut niveau.

On répond ainsi au besoin de garantir l'identité des AC ministérielles : cela permet notamment aux ministères qui n'ont pas les moyens de mettre en œuvre une politique lourde de publication d'apporter à un tiers (autre ministère, organisme privé ou étranger) la garantie nécessaire à l'établissement d'une relation de confiance.

Dans une étape ultérieure et toujours à l'initiative des ministères, ce service de certification pourrait être étendu et contribuer à la réalisation d'un véritable *pont de confiance (Bridge-CA*) reliant les différentes autorités de certification ministérielles. Ce concept, précisé dans la suite du document (§4), nous rapproche de la proposition de M. Carcenac.

Les registres d'IGC

Les registres ministériels

Les ministères volontaires tiennent un registre ministériel, placé sous la responsabilité du haut fonctionnaire de défense, contenant notamment les politiques de certification et les déclarations des pratiques de certification, ainsi que les certificats racines pour chacune des IGC déployées.

Le registre interministériel

Ce registre géré par la DCSSI contient les données des registres ministériels relatives aux IGC faisant l'objet d'accords de reconnaissance avec des organismes extérieurs à leur ministère d'origine. Il peut contenir

également les données de toute IGC que souhaiteraient déclarer les ministères, même hors du cadre d'un accord interministériel.

Validation des accords de reconnaissance

La méthodologie préconisée repose sur l'établissement d'un accord de reconnaissance qui précise les conditions autorisant une ou plusieurs IGC à gérer des certificats d'IGC utilisés pour sécuriser des échanges électroniques entre les parties prenantes de cet accord.

Les PC et les DPC des IGC identifiées dans l'accord sont d'abord enregistrées au registre interministériel. Le dossier de validation est remis au SGDN par les autorités de sécurité des IGC parties prenantes. Le SGDN vérifie la cohérence entre les objectifs et les exigences de sécurité des éléments du dossier de validation en comparant les politiques de certification des IGC donnant lieu à l'accord.

Le SGDN procède ensuite à la vérification de la réalisation des objectifs de sécurité déclarés dans les PC en les mettant en correspondance avec les pratiques déclarées. À l'issue de ces vérifications, il peut valider l'accord ou proposer des actions correctives.

L'autorité nationale de certification

L'autorité de certification IGC/A répond aujourd'hui au besoin de garantir l'identité des autorités de certification de plus haut niveau. Elle ne délivre pas de certificats aux utilisateurs au sein des ministères, mais seulement à ces autorités racines ministérielles, à leur demande.

Cette disposition ouvre toutefois des perspectives nouvelles (esquissées dans la proposition n° 31 du rapport Carcenac) visant la simplification de la constitution d'un réseau de confiance entre plusieurs entités. Si la certification d'une AC ministérielle au niveau national se double d'un accord générique pris entre l'AC ministérielle et l'AC nationale, on peut imaginer de pouvoir se dispenser dans certains cas d'accords de reconnaissance entre ministères.

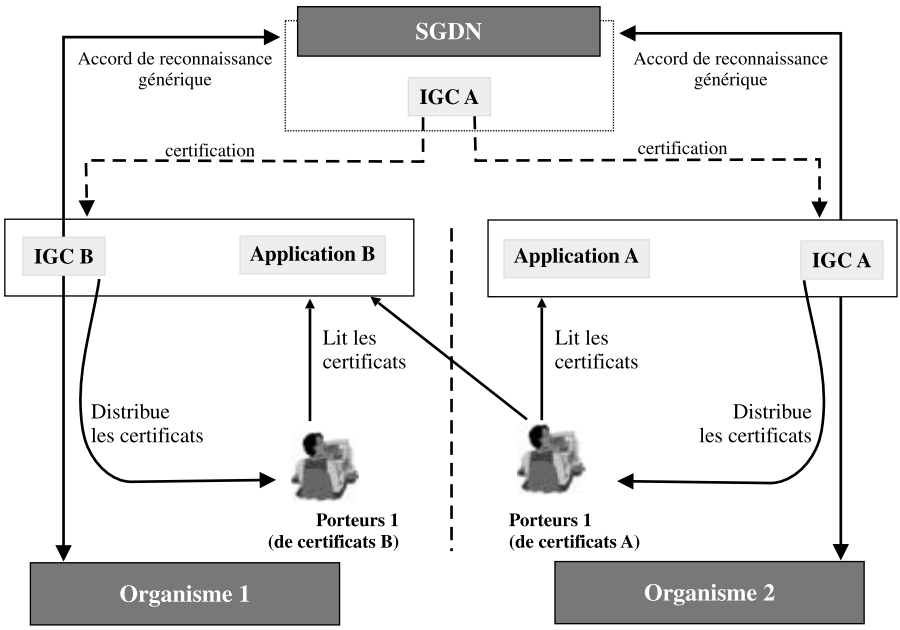
Cet accord pris avec l'AC nationale serait général, sans viser d'applications précises, en définissant des classes et des niveaux d'exigence. On peut imaginer un gain important : par exemple dans le cas d'une messagerie reliant 10 ministères et sécurisée par les certificats issus de 10 AC ministérielles, les AC devraient s'accorder deux à deux ce qui nécessiterait 45 comparaisons techniques de PC et DPC, alors qu'en passant par

un « *pont de confiance* » (l'AC nationale, qui joue donc le rôle de *bridge-CA*) seuls 10 accords génériques seront nécessaires.

Le schéma ci-dessous illustre la chaîne de confiance établie entre un porteur 2 et l'application B. L'application B peut autoriser l'exécution d'une requête émise par le porteur 2 car tous les deux partagent un même point de confiance, l'IGC/A, qui aura préalablement certifié les autorités de certification A et B, sur la base d'accords généraux.

Dans cet esprit, l'IGC/A actuelle (limitée à l'identification d'AC) pourrait évoluer à moyen terme, si ce besoin se confirmait, vers une deuxième phase où elle deviendrait un véritable pont de confiance entre administrations. L'IGC/A pourrait alors produire des certificats et des listes de révocation qui pourront être publiés sur un méta-annuaire interministériel ou sur internet pour satisfaire les besoins des ministères et des utilisateurs finaux.

L'intérêt de disposer d'un tel « pont de confiance » peut être illustré par l'exemple de la certification de serveurs applicatifs SSL des administrations. Il pourrait être envisagé que le SGDN négocie avec les éditeurs de logiciel l'inclusion par défaut dans leurs produits d'une clé publique de l'IGC/A. De cette manière, l'ensemble des serveurs SSL des administrations pourraient être reconnus par les navigateurs du marché. (Une telle démarche aurait certainement beaucoup plus de chance de réussir que si chaque ministère essayait de négocier séparément avec les éditeurs.)



La problématique de la sécurité des systèmes d'information (SSI)

Contribution de la DCSSI

Le gouvernement s'est engagé depuis 1997 dans le domaine de l'administration électronique, qui est l'un des axes prioritaires du programme d'action gouvernemental pour la société de l'information (PAGSI). Il s'agit de mettre les technologies de l'information au service de la modernisation des services publics, d'améliorer l'efficacité de l'action des administrations de l'État comme des collectivités locales et la qualité des relations entre celles-ci et leurs usagers. Cette dématérialisation des services publics ne peut s'effectuer sans une attention accrue portée à la sécurité. Au sein de du secrétariat général de la Défense nationale (SGDN), la direction centrale de la sécurité des systèmes d'information (DCSSI) contribue à la définition interministérielle et à l'expression de la politique gouvernementale en matière de sécurité des systèmes d'information (SSI), et assiste les services publics dans sa mise en œuvre.

La problématique SSI

Dans un environnement en évolution permanente sur les aspects techniques, légaux, organisationnels et commerciaux, les menaces qui pèsent sur les systèmes d'information (SI) doivent être constamment réévaluées. La menace peut être ludique (de plus en plus d'outils d'attaque automatiques sont accessibles par internet), avide, stratégique ou terroriste ; elle peut faire intervenir des attaquants qui exploitent les vulnérabilités des matériels et des logiciels, mais aussi des réseaux, des sites, des organisations et des personnels. Ainsi, un équilibre doit être recherché entre ces menaces d'une part, et d'autre part, le niveau de confiance que l'on veut accorder à son système d'information en exprimant ses besoins, en gérant ses objectifs de sécurité, en précisant ses exigences fonctionnelles et d'assurances.

La gestion du risque

Cet équilibre repose sur l'analyse et sur la gestion des risques en matière de sécurité des systèmes d'information. Cette démarche doit être menée globalement, non seulement selon des domaines (matériels, logiciels, personnels, infrastructures, etc...), mais aussi en termes de cycle de vie du SI (conception, réalisation, installation, maintenance, évolution, fin de vie) et dans une dynamique de conduite du changement, tout en respectant les réglementations en vigueur. Cette vision d'ensemble du SI donne du sens au projet de sécurité au travers de concepts partagés, d'une sensibilisation de l'ensemble des utilisateurs et d'une implication des acteurs. Cependant, conduire une démarche de gestion du risque est difficile car :
– chaque personne appréhende les risques d'une façon différente en fonction de sa perception des valeurs de l'entreprises, de ses missions, de son propre vécu ;
– le risque est uniquement un phénomène à venir et le temps affecte la perception du risque car plus l'échéance est lointaine, plus le degré d'incertitude est important.
La DCSSI a développé la méthode **EBIOS** ® (Expression des besoins et identification des objectifs de sécurité) fournissant aux maîtrises d'ouvrages une démarche globale, afin de prendre en compte la sécurité au sein des projets de création ou d'évolution des SI. La méthode est articulée autour de quatre étapes :
– le contexte : environnement du SI, détermination de la cible de l'étude ;
– les besoins : définition de la sensibilité des informations ;
– les risques : détermination des risques spécifiques du SI et confrontation aux besoins ;
– l'expression des objectifs de sécurité.

Éléments de sécurisation d'un SI

L'intégration de la SSI dans la gestion de projet au travers d'une étude de gestion de risques comme EBIOS ®, permet de définir un cadre de développement de systèmes d'information sécurisés. Ainsi, en fonction de la finesse de l'étude, les maîtrises d'ouvrages ont la possibilité d'exploiter les résultats de la démarche afin de rédiger des politiques de sécurité des systèmes d'information (PSSI), de concevoir des plans de sécurité ou des schémas directeurs, d'écrire des fiches d'expression rationnelle des objectifs de sécurité (FEROS) ou encore des profils de protection (PP au sens de l'ISO 15408).
Parallèlement à ces documents de référence et à leur mise en œuvre, la tenue de tableaux de bords orientés vers le contrôle de la sécurité participe à la SSI. Ces outils regroupent des indicateurs rendant compte de la sécurité des systèmes d'information sur les plans de la disponibilité, de l'intégrité et de la confidentialité des informations et des applications. Un tableau de bord permet de suivre différents éléments clés tels que la qualité de la politique de sécurité, les services de sécurité, les actions ou les alertes. Il couvre les domaines technique, organisationnel et juridique. Un tableau de bord constitue un outil de synthèse et de visualisation indispensable, mais s'avère toujours difficile à mettre en place.

Enfin, le concept de la défense en profondeur est utilisé dans le cadre de la gestion du risque. Ce concept s'appuie, entre autres, sur la définition de lignes de défense et sur l'indépendance de ces lignes. La défense en profondeur se traduit dans un SI par une succession de barrières reposant sur des technologies différentes et structurant le système autour d'enclaves. Cette architecture, associée au principe de redondance des moyens de protection et de sauvegarde, optimise la sécurisation du SI.

Pour une prise en compte globale de la SSI

Dans tous les projets d'administration électronique figure une composante sécurité. Cette sécurité sera d'autant mieux prise en compte, dans des conditions financières, calendaires et humaines optimales, qu'elle est intégrée dès l'origine dans la gestion des projets et qu'elle est assumée au plus haut niveau hiérarchique comme une composante stratégique.

Les projets de téléservices du ministère de l'Intérieur

Contribution du ministère de l'Intérieur – DLPAJ – Michel Aubouin – novembre 2001

Le ministère de l'Intérieur a développé une série de téléservices qui concernent à la fois l'administration centrale et les préfectures. Les projets portés par les préfectures, en vertu du principe de la déconcentration, revêtent souvent un caractère interministériel.

Il s'agit, selon le cas, de projets, d'expérimentations ou de réalisations.

La télétransmission des actes des collectivités locales

Cette expérimentation, conduite par la DGCL, s'inscrit dans un contexte de forte hausse du nombre d'actes transmis au titre du contrôle de légalité. Elle a été menée au 1er trimestre 2001 sur quatre sites, dans les départements des Yvelines, du Rhône, de la Saône-et-Loire et des Deux-Sèvres, en association étroite avec l'Association des maires de France et l'Association des départements de France.

Elle a porté sur une partie des actes transmis, les actes simples tels que les délibérations et les arrêtés. Les transmissions électroniques, empruntant le réseau internet, ont été sécurisées par un procédé de signature électronique, l'utilisation d'une carte à puce (certificats résidant sur une carte à microprocesseur) s'étant avérée la plus commode. La carte n'est utilisée que pour se connecter au serveur et, par là même, authentifier l'émetteur. Les actes étaient conservés sur un serveur unique. S'agissant d'une expérimentation, la procédure de transmission par voie informatique n'a pas supprimé la transmission ordinaire par courrier.

L'évaluation de la méthode a été conduite par l'inspection générale de l'administration. Plusieurs enseignements ont été dégagés :
– la faculté de transmettre les actes sous cette forme doit être laissée aux communes, en vertu du principe de la libre administration des collectivités locales ;

– la qualité du signataire doit être définie : est-ce un élu (le maire) qui signe la transmission ? Doit-elle être signée ? Quid des délégations de signature ?
– le choix de la certification est-il libre ou encadré ? (question de standard, référencement...). Qui doit assumer la gestion des certificats ?
– le problème de l'horodatage doit être résolu. Est-ce que l'heure de transmission fait courir les délais contentieux, alors même que la préfecture peut ne pas avoir reçu le document ?
– la diversité des formats utilisés complexifie leur traitement ;
– le problème de l'archivage mérite une réflexion spécifique. Est-il local ou national ? Qui en est responsable ? Qui le finance ? pour quel durée et sur quel support ?
– la relation avec les autres ministères n'est pas résolue (le Trésor public, par exemple, a besoin des actes à l'appui des ordonnancements).

La transmission dématérialisée des actes budgétaires est à l'étude. Elle présenterait un grand intérêt associée au développement de logiciels d'aide au contrôle, de traitements statistiques ou d'analyse financière. Une discussion est en cours avec la comptabilité publique.

La télétransmission des documents de nature complexe (les documents d'urbanisme par exemple, qui utilisent des plans) et des documents revêtus de la signature de tiers (dans le cadre des marchés publics) supposent la résolution préalable de difficultés techniques actuellement examinées.

L'intérêt de cette procédure réside évidemment dans l'utilisation conjointe d'outils d'aide au contrôle. Une réflexion est engagée sur le nombre et la nature des actes à transmettre, la limite de la dématérialisation des actes restant liée aux obligations d'affichage.

L'expérience conduite en 2001 va être étendue en 2002. Les associations d'élus (A.M.F. et A.D.F.) seront associées à l'ensemble du processus. La CNIL sera saisie du problème spécifique des informations personnelles traitées dans le cadre du contrôle des actes individuels. Une norme technique de transmission pourrait être élaborée, peut-être associée à une convention-type signée entre la préfecture et les collectivités.

Il est à noter qu'il n'existe pas encore de jurisprudence sur la dématérialisation des actes soumis au contrôle de légalité.

La télétransmission des dossiers de cartes grises

Près de 13 000 000 de titres sont délivrés par an. La télétransmission des dossiers a été mise en place dès 1994 ; elle a été progressivement étendue. Il s'agit d'une procédure impliquant un tiers : un constructeur, un loueur ou un concessionnaire, agissant par délégation pour saisir les données relatives au véhicule et à l'acquéreur.

L'échange des données informatisées concerne donc les relations entre le ministère de l'Intérieur, ses partenaires du secteur public

(comptabilité publique, gendarmerie nationale) et ceux du secteur privé (constructeurs, loueurs, démolisseurs, assurances...). Les opérations en cause sont les immatriculations de véhicules neufs, les inscriptions de déclaration d'achat, de destruction et de cession.

En 2000, l'immatriculation des véhicules neufs par télétransmission a représenté près de 47 % des immatriculations (90 % des véhicules neufs des marques Peugeot et Citroën, 60 % pour la marque Renault). Les marques étrangères rejoignent progressivement les constructeurs français.

En ce qui concerne les véhicule d'occasion, le potentiel est d'environ 3 000 000 de transactions par an traitées chez les concessionnaires. Le même nombre de véhicules est vendu dans des relations directes entre particuliers qui échappent par nature, pour l'instant, à cette procédure de télétransmission.

Plusieurs difficultés peuvent être signalées :

• Seuls les partenaires importants, représentant des flux significatifs, peuvent échanger directement avec l'application nationale, car ces transactions exigent l'utilisation de liaisons spécialisées. Les autres se regroupent autour de R.V.A. (réseaux à valeur ajoutée), mais la gestion des accès à des R.V.A. qui se multiplient induit des difficultés techniques.

• La gestion de la clientèle demeure complexe pour les entreprises. Une partie de la procédure technique est déplacée chez le partenaire, ce qui entraîne un système de validation, d'habilitation des émetteurs et de maintenance assez lourd.

• Les coûts induits peuvent paraître élevés.

• Le système manque sans doute de flexibilité et l'interopérabilité est difficile.

Une étude de faisabilité va être engagée en ce qui concerne les accès directs des usagers. On en attend les premiers développements dans un an. La signature électronique devrait permettre le développement de la téléprocédure. Dans le même temps, on assiste au développement de normes internationales afin de favoriser les échanges entre les partenaires européens.

La procédure de télépaiement est actuellement à l'étude en liaison avec la Comptabilité publique.

La télétransmission des permis de conduire

Un projet expérimental relatif au permis de conduire a été testé dans le département de la Haute-Vienne, en relation avec deux auto-écoles. Il s'agit de l'envoi par téléprocédure de l'inscription à l'auto-école et de la notification de la réussite à l'examen final, afin d'éviter le travail de saisie des préfectures. Une étude technique est en cours concernant le raccordement de ces auto-écoles au fichier du service national du permis de conduire.

Le titre-fondateur

La réflexion engagée par le ministère de l'Intérieur ne porte pas à proprement parler sur la conception d'un téléservice, mais plutôt sur la création d'un outil d'authentification et de signature (la carte nationale d'identité électronique) susceptible de faciliter les téléprocédures. Les automatisations qui en découleront concerneront les services en ligne, mais surtout, dans un premier temps, l'accès aux formulaires et aux documents sur des bornes interactives.

Il existe d'ailleurs déjà, dans les halls des préfectures, les bornes de non-gage. Les services rendus par des bornes de ce type peuvent être étendus et il est envisagé de les rendre accessibles à tout moment, sur le modèle des automates bancaires.

Les autres téléservices

Toutes les préfectures se sont dotées de sites internet qui fournissent des renseignements administratifs, proposent des formulaires en ligne et effectuent des renvois sur le site « service.public.fr ».

Des sites locaux à vocation interministérielle (sites « portail ») sont également développés.

Les formulaires sont en général disponibles en téléchargement mais plusieurs préfectures testent des services plus avancés (la Haute-Vienne par exemple), où l'usager saisit les données qui le concernent et reçoit par courrier le document sollicité.

Le programme Copernic : identification des contribuables et protection des données personnelles

Contribution du MINEFI
Audition de M. Grapinet, directeur
du programme Copernic – 26 novembre 2001

Le ministère de l'Économie, des Finances et de l'Industrie (MINEFI) a lancé dans le cadre de sa réforme – modernisation un programme baptisé COPERNIC axé sur la transformation en profondeur des outils informatiques des administrations fiscales. Le plan d'action, approuvé par le ministre au début de l'année 2001, a pour objectif de mettre à disposition des contribuables, via une large palette de moyens de communication, des outils nouveaux pour une gestion globale, cohérente et facilitée de leur situation fiscale.

S'appuyant massivement sur l'apport des technologies de l'information et de la communication, le programme Copernic vise la mise en place à terme d'une véritable « e-administration fiscale » sans papier, multimédia et multiservices.

Conduit en commun par la direction générale des Impôts et la direction générale de la comptabilité publique, le programme COPERNIC implique la refonte en profondeur des systèmes d'information de ces deux directions pour surmonter les divers cloisonnements qui empêchent les échanges d'informations entre elles et nuisent à la qualité des services délivrés aux usagers. Parallèlement à cet effort de mise en cohérence dans la durée, l'organisation des travaux a été conçue pour apporter régulièrement des progrès visibles pour les usagers et les agents dès 2002.

Développer une offre de services diversifiée et « multicanaux »...

Dans le cadre des études Copernic, une première série de projets (une soixantaine) a été identifiée dont la moitié directement destinée à offrir des services nouveaux aux usagers et aux agents.

Il en est ainsi de services à distance qui permettront à terme d'offrir au contribuable une gestion intégralement dématérialisée de ses affaires fiscales depuis son domicile ou son entreprise, avec une étape significative dans les prochains mois pour la déclaration et le paiement de la plupart des principaux impôts. Les services délivrés par téléphone seront notablement renforcés par la généralisation d'impôts-service en 2003, après une extension en 2002.

Les moyens d'accès traditionnels seront améliorés, notamment le guichet où le décloisonnement des bases informatiques permettra d'obtenir une information plus complète auprès des agents et où les contribuables pourront également trouver des bornes interactives (quatre sont en cours d'expérimentation) ou des postes internet en libre service.

Ainsi, l'ensemble des données relatives à la situation fiscale d'un usager – particulier ou entreprise – sera accessible aux agents des deux réseaux et mis à disposition du contribuable concerné, via internet par exemple. De cette façon, chaque contribuable pourra disposer de l'ensemble des informations concernant ses différents impôts et communiquer avec l'administration fiscale par les moyens de son choix.

L'ouverture du portail fiscal constitue une première étape significative dans l'objectif de mise à la disposition des usagers de nouveaux services. Depuis le 11 mars 2002, il est ainsi possible de déclarer ses revenus sur internet et d'accéder à son dossier fiscal dans des conditions de haute sécurité grâce au recours au certificat et à la signature électroniques.

Par la suite, l'offre de services continuera à se développer en apportant des prestations plus personnalisées. À terme, le « compte fiscal simplifié » devrait permettre aux usagers d'avoir accès, à leur demande, à l'ensemble des informations concernant leur situation personnelle. Ils pourront bénéficier d'un calendrier fiscal propre leur signalant, par envoi de message électronique, l'approche des dates limites de déclarations ou de paiement. Ils pourront également demander des compensations entre leurs différents impôts.

… en veillant tout particulièrement au respect des libertés publiques

Le programme Copernic a, dès son lancement, identifié la protection des données personnelles comme un enjeu majeur.

L'élaboration d'une politique globale de sécurité et le recours aux technologies les plus avancées telles que, notamment, le cryptage, les points d'accès sécurisés renforcés ou l'authentification par certificat électronique offrent des garanties de très haut niveau.

Dans le même temps, l'accès aux données personnelles est rigoureusement contrôlé par l'authentification des utilisateurs (agents comme usagers). Une gestion fine des habilitations délivrées aux personnels de l'administration doublée d'un contrôle *a posteriori* fondé sur la tra-

çabilité des consultations effectuées renforce le contrôle interne sur les données examinées.

De plus, le système d'information cible est centré sur les personnes afin de mieux les distinguer d'entités plus complexe comme celles de foyers fiscaux ou d'indivision. Il permet de réserver à chacun l'information qu'il est en droit de connaître. Ainsi, au sein d'un couple marié sous le régime de droit commun, les époux ont accès tous deux aux informations concernant leur déclaration commune de revenus, mais seul le conjoint propriétaire en propre d'un bien immobilier pourra consulter les données relatives à ce dernier.

Ce choix d'organisation permet de faciliter l'exercice du droit d'accès et de rectification reconnu par la loi relative à l'informatique, aux fichiers et aux libertés du 6 janvier 1978, l'usager pouvant restreindre de lui-même son accès à certains des services qui lui sont offerts.

Par ailleurs, le programme Copernic travaille en liaison étroite avec la CNIL. Outre le dépôt de demande d'avis ou de déclaration de modification des traitements automatisés d'informations nominatives pour lesquels un avis motivé de cette commission est nécessaire, un dialogue continu a été instauré.

Les axes stratégiques du programme et des projets sont présentés en amont afin d'assurer une meilleure visibilité de l'ensemble de la démarche élaborée. Les questions liées à la sécurité feront l'objet, si nécessaire, de présentations spécifiques.

De plus, les directeurs généraux de la direction générale des Impôts et de la direction générale de la Comptabilité publique ont proposé d'assurer un point annuel en séance plénière de la Commission nationale de l'informatique et des libertés.

En offrant de nouveaux services, dans le respect des droits des citoyens et en veillant à l'encadrement des pouvoirs de l'administration, le programme Copernic doit permettre de renforcer le civisme fiscal. Si Copernic ne peut pas rendre l'impôt plus agréable, il aspire à le rendre plus facile à vivre.

Net-entreprises

Contribution du GIP-MDS

Net-entreprises est le service de télédéclarations sociales sur internet proposé aux entreprises par l'ensemble des organismes de protection sociale. Il s'agit d'un service gratuit, facultatif, chaque entreprise pouvant l'utiliser pour tout ou partie des déclarations qui la concernent.

Ce projet concerne toutes les entreprises. Quels que soient leur taille (90 % d'entre elles ont moins de dix salariés), leur secteur d'activité ou leur implantation géographique, elles peuvent s'acquitter de leurs obligations déclaratives vis-à-vis des organismes de protection sociale (OPS) en utilisant le média internet. Les experts comptables, qui effectuent pour le compte de leurs clients presque la moitié de l'ensemble des 130 millions de déclarations sociales produites chaque année, peuvent également utiliser Net-entreprises.

La sécurité est un élément central dans Net-entreprises. Elle conditionne en effet la confiance des entreprises dans l'utilisation du service. Les besoins de sécurité ne sont pas spécifiques, mais sont différents entre déclarations. On peut néanmoins les regrouper en deux grandes catégories : la confidentialité des données échangées et stockées et l'intégrité de ces données. Le contrôle d'accès est l'élément central de la confidentialité. Il se décline lui-même en identification (qui est l'internaute ?) et en authentification (peut-il prouver son identité et son habilitation à accéder au service de déclaration, de paiement, de consultation des anciennes déclarations ?). L'intégrité (l'administration a-t-elle bien reçu ce que j'ai envoyé ?) est garantie notamment par l'accusé de réception.

Net-entreprises utilise actuellement un identifiant associé à un mot de passe non trivial, et les liaisons sont sécurisées (SSL 128 bits). C'est suffisant dans l'immédiat, mais une migration vers des systèmes offrant un meilleur niveau de sécurité est planifiée. La décision a été prise en avril 2001 de se mettre en état d'accepter les certificats électroniques du marché (Télé-TVA et carte de professionnel de santé), pour garantir une authentification forte des personnes physiques accédant à Net-entreprises pour le compte de leur entreprise, et permettre la signature électronique des déclarations et règlements. Cela sera opérationnel vers la mi-2003. Cependant, le prix des certificats du marché laisse craindre l'absence de leur diffusion massive, notamment aux plus petites entreprises, aboutissant à une sécurité à deux vitesses. Par ailleurs, les failles actuelles dans les sys-

tèmes d'identification (homonymies, difficulté du choix entre nom patronymique et nom d'usage, révocation des certificats au moment du décès des personnes) ont incité la sphère sociale à s'interroger sur l'opportunité qu'elle délivre gratuitement des certificats électroniques permettant d'accéder aux services qu'elle propose (télédéclarations sociales, accès aux anciennes déclarations, mais aussi accès aux comptes au sein de chaque OPS, etc.), les outils diffusés pouvant éventuellement être utilisés pour des téléservices d'autres administrations.

Les questions techniques, organisationnelles et économiques, non totalement cernées à ce stade, ont conduit la sphère sociale à prévoir une expérimentation préalable à toute décision de généralisation. Une telle expérimentation devrait intervenir à l'automne 2003, avec une évaluation au printemps 2004. La décision définitive serait prise sur la base de cette évaluation.

Les auteurs

Pierre TRUCHE, magistrat, a été notamment premier président de la Cour de cassation (1996-1999) et président de la Commission nationale consultative des droits de l'homme (1999-2001). Il est aujourd'hui président de la Commission nationale de déontologie des forces de sécurité.

Jean-Paul FAUGÈRE est ancien élève de l'ENA et conseiller d'État. Il a été notamment directeur des libertés publiques et des affaires juridiques au ministère de l'Intérieur (1994-1997). Il est aujourd'hui préfet de la Vendée.

Patrice FLICHY est professeur de sociologie à l'université de Marne-la-Vallée et a notamment dirigé pendant quinze ans le laboratoire de sociologie du Centre national d'étude des télécommunications (CNET). Directeur de la revue *Réseaux, communication, technologie et société*, il a également publié en octobre 2001 *L'imaginaire d'internet* (éditions La Découverte).