Date de dépôt : 2 avril 2015

Rapport du Conseil d'Etat
au Grand Conseil sur l'Administration en ligne sous l'angle de la LIPAD

Mesdames et
Messieurs les députés,

Préambule

Contexte

Le Grand Conseil a voté le 26 juin 2008 la loi 10177[1], qui a ouvert un crédit d'investissement de 26 350 000 F pour financer le projet d'Administration en ligne (AeL).

Ce projet visait à mettre en place une infrastructure commune, harmoniser les registres de personnes conformément à la loi fédérale sur l'harmonisation des registres des habitants et d'autres registres officiels de personnes, du 23 juin 2006 (LHR – RS 431.02) et à sa loi cantonale d'application (LaLHR – rs/GE F 2 25) et à réaliser dix prestations en ligne initiales (les prestations d'impulsion) ainsi que neuf prestations complémentaires[2]. S'y ajoutaient l'accompagnement de ces mesures auprès de la population et celui du changement au sein de l'administration.

La réalisation de ces objectifs nécessitait :

– l'offre d'un système d'identification et d'authentification standardisé;
– l'élaboration des composants techniques transversaux nécessaires au déploiement et au fonctionnement de l'ensemble des prestations;

---

[1] *L 10177, loi ouvrant un crédit d'investissement de 26 350 000 F pour le développement de l'administration en ligne, Genève, 26 juin 2008,* (http://www.ge.ch/grandconseil/data/loisvotee/L10177.pdf).

[2] *PL 10177, projet de loi ouvrant un crédit d'investissement de 30 850 000 F pour le développement de l'administration en ligne, Genève, 28 novembre 2007, pp. 8-9 (http://www.ge.ch/grandconseil/data/texte/PL10177.pdf); projet de loi de bouclement de la loi 10177 ouvrant un crédit d'investissement de 26 350 000 F pour le développement de l'administration en ligne.*

ATAR ROTO PRESSE – 200 ex. – 05.15

– une identité visuelle globale, sans aucune forme d'exclusion;
– le développement de partenariats internes et externes pour accompagner une nouvelle façon de travailler tenant compte des prestations en ligne[3].

On comprend, à la lecture de ce qui précède, que l'Administration en ligne ne porte pas que sur le seul déploiement de diverses prestations accessibles via Internet : elle entraîne une refonte transverse de l'ensemble des systèmes d'information de l'Etat. La loi sur l'information du public, l'accès aux documents et la protection des données personnelles, du 5 octobre 2001 (ci-après : LIPAD) a fait l'objet d'un article spécifique, l'article 69, illustrant cet impératif et ce caractère transversal de l'Administration en ligne.

Ce caractère expérimental prendra fin le 31 décembre 2015.

Les hasards du calendrier veulent que lors de sa séance du 4 décembre 2014, le comité de pilotage de la cyberadministration suisse a commandé une planification des projets-clés suisses dès 2016. Ce comité de pilotage a adopté les objectifs globaux de la coopération en matière de cyberadministration en les plaçant sous la devise « *La cyberadministration va de soi : des prestations administratives rapides, transparentes et efficientes fournies en ligne à la population, aux acteurs économiques et au secteur public* ». En outre, le comité de pilotage complète le catalogue des projets prioritaires par le projet « B1.16 Gestion des connaissances juridiques pour la cyberadministration », qu'il intègre par la même occasion dans le plan d'action 2015[4]. Les décisions stratégiques de notre canton en matière de prestations en ligne ne peuvent ignorer ce programme et le présent rapport tient également compte de ce paramètre.

Buts du rapport

A teneur de l'article 69, alinéa 8 LIPAD, trois rapports d'évaluation doivent être remis au Grand Conseil. Celui du Conseil d'Etat doit pour sa part :

– indiquer, pour chacune des 10 prestations d'impulsion prioritaires du programme d'administration en ligne, si, dans quelle mesure et pourquoi leur développement, leur exploitation ou leur évolution ont impliqué un recours à la disposition dérogatoire contenue dans l'article 69 LIPAD;

[3] *PL Bouclement 10177, op. cit, p. 9.*

[4] *https://www.news.admin.ch/message/index.html?lang=fr&msg-id=55576*

– établir une évaluation des effets de l'expérience conduite en considération :
  a) des contraintes techniques et opérationnelles de l'administration;
  b) des buts de la LIPAD;
  c) des besoins des utilisateurs, de l'utilité et de la fréquence du recours aux solutions offertes au public.
– proposer si nécessaire un projet de loi visant à ancrer durablement dans la législation tout ou partie des éventuelles dérogations qui s'imposent.

Selon l'exposé des motifs relatif à l'article 69 LIPAD[5], à l'expiration de la disposition expérimentale, il sera possible de déterminer la nécessité de déroger aux principes de la LIPAD pour ancrer durablement dans la législation les prestations en ligne offertes. « *Si la réponse devait s'avérer négative, la disposition dérogatoire sera de plein droit abrogée et il conviendra alors d'adapter, de réduire ou de supprimer un certain nombre de prestations en ligne, en renonçant à toute dérogation à la LIPAD. Si à l'inverse, cette réponse devait être affirmative, il suffira alors d'indiquer dans la loi elle-même et dans la stricte mesure de ce qui aura été jugé comme nécessaire, les dérogations qui s'imposent en fonction des prestations spécifiques évoluées, soit en mentionnant ces exceptions dans la loi générale qu'est la LIPAD, soit en modifiant d'éventuelles législations spéciales* »[6].

L'expérience acquise au cours du programme AeL montre que les alternatives envisagées par l'article 69 LIPAD ont changé : alors que la nécessité de déroger aux principes de la LIPAD pour ancrer durablement dans la législation les prestations en ligne offertes ne se fait pas sentir, sans que cela implique d'adapter, de réduire ou de supprimer un certain nombre de prestations en ligne, c'est la question même du **contrôle de la conformité à la LIPAD qui doit être abordée**. C'est sous cet angle qu'il s'agit de prendre la mesure du changement que les e-démarches – c'est le nom qui a été donné depuis lors aux prestations en ligne – entraînent.

Le présent rapport se propose donc d'exposer les initiatives que l'AeL a menées afin de respecter les principes de la LIPAD ainsi que les difficultés rencontrées à cette occasion, avant de s'ouvrir sur des propositions permettant à l'avenir d'assurer de manière uniforme et dès leur conception la conformité à la LIPAD des prestations en ligne.

---

[5] *Projet de loi modifiant la loi sur l'information du public, l'accès aux documents et la protection des données personnelles (LIPAD) (A 2 08), PL 10555.*

[6] *PL 10555, op. cit., exposé des motifs, p. 7.*

Liste des principaux acronymes utilisés

AeL	Administration en ligne (programme d'impulsion)
AFC	Administration fiscale cantonale genevoise
CGSIC	Comité de gouvernance des systèmes d'information et de communication
CGU AeL	Conditions générales d'utilisation des sites de prestation en ligne de l'administration genevoise
CP	Code pénal suisse
DGSI	Direction générale des systèmes d'information
DSE	Département de la sécurité et de l'économie
GAPP	*Generally Accepted Privacy Principles (voir PPRP ci-dessous)*
GSU	Guichet sécurisé unique de l'administration neuchâteloise
ICIA	*Information Confidentiality Impact Assessment*
LGSU	Loi sur le guichet sécurisé unique (rs/NE 150.40)
LIPAD	Loi sur l'information du public, l'accès aux documents et la protection des données personnelles (rs/GE A 2 08)
LPD	Loi fédérale sur la protection des données (RS 235.1)
LAeL	Loi sur l'Administration en ligne (LAeL, projet)
OCEN	Office cantonal de l'énergie
OCPM	Office cantonal de la population et des migrations
OROI	Office départemental responsable de l'organisation de l'information
PFPDT	Préposé fédéral à la protection des données et à la transparence
PPDT	Préposé(e) genevois(e) à la protection des données et à la transparence
PPRP	Principes généralement reconnus en matière de protection des renseignements personnels (en anglais « *Generally Accepted Privacy Principles* » – GAPP)
RC	Registre du commerce du Canton de Genève
RCEL	Règlement genevois sur la communication électronique (rs/GE E 5 10.05 – RCEL)
RDIOI	Règlement genevois relatif aux déclarations d'impôt établies à l'aide d'outils informatiques (rs/GE D 3 17.03)
RF	Registre foncier genevois

RIPAD	Règlement d'application de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles (rs/GE A 2 08.01)
ROGSIC	Règlement sur l'organisation et la gouvernance des systèmes d'information et de communication (rs/GE B 4 23.03)
RS	Recueil systématique des lois fédérales
rs/GE	Recueil systématique des lois genevoises
rs/NE	Recueil systématique des lois neuchâteloises
RSI	Responsable départemental de la sécurité de l'information (rôle instauré par le ROGSIC)
SGPD	Système de gestion de la protection des données
SI	Système d'information
SIPD	Sûreté de l'information et protection des données
TIC	Technologies de l'information et de la communication
TICIA	*Tax Information Confidentiality Impact Assessment*

Définition des principales notions

Plusieurs notions essentielles méritent d'être explicitées, afin de mieux comprendre le présent rapport et les difficultés rencontrées par la mise en œuvre de la LIPAD dans ce contexte.

Administration en ligne

Bien que l'article 69 LIPAD fasse expressément référence aux dix prestations d'impulsion prioritaires, le programme de l'AeL a mis en service d'autres prestations. La mise en œuvre de ces prestations a soulevé des problématiques essentiellement transverses, ce qui explique l'approche du présent rapport. Ce dernier intègre dans sa réflexion l'ensemble des prestations en ligne, qu'elles soient présentes ou futures.

Prestations en ligne

Une prestation en ligne est un service offert par un office (en application d'une loi ou d'un règlement), délivré à travers un canal numérique à un utilisateur externe à l'Etat. A ce titre, les contenus des prestations en ligne sont de nature essentiellement transactionnelle, qui suppose un échange d'informations entre l'administration et le citoyen. Cela les distingue des simples contenus informationnels; au sens du présent rapport, la délivrance d'une simple information générale par le biais d'un site Internet – le portail de l'Etat par exemple – n'est donc pas considérée comme une prestation en ligne.

La notion de prestation en ligne est plus large que celle de prestation délivrée dans le cadre du programme de l'AeL, même si l'AeL ne se limite pas aux seules dix prestations d'impulsion. De fait, quelques prestations en ligne ont été développées sans le financement du programme AeL.

Il convient enfin de préciser que l'expression de « prestation en ligne » a été remplacée par le terme « e-démarche ».

Données et information

Les notions de *donnée* et d'*information* sont comprises de manière souvent contraire par les informaticiens et par les juristes. Alors que pour la LIPAD – et donc les juristes – la donnée représente la forme brute, sans mise en contexte ni interprétation, de l'information, c'est l'information qui, pour les théories de l'information, devient « donnée » par sa mise en contexte[7]. Ainsi, les mesures brutes et les relevés d'observation constituent pour les informaticiens de simples données, alors qu'une mise en contexte (les fameux « liens » des bases de données relationnelles) s'avère nécessaire pour en faire des informations. Pour les juristes au contraire, les informations, pour devenir données (personnelles), doivent être mises en relation (avec une personne), si bien par exemple qu'un modèle de véhicule ne constitue une donnée personnelle qu'à partir du moment où il se trouve relié à un propriétaire.

Le caractère diamétralement opposé de ces deux approches génère de nombreux quiproquos dont il faut tenir compte, en particulier dans le cadre de la mise en conformité à la LIPAD par l'AeL où ces deux métiers sont appelés à collaborer étroitement. Cette opposition terminologique est levée par l'expression *renseignements personnels,* retenue par le référentiel internationalement reconnu en matière de contrôle de la conformité de la protection des données (PPRP ou GAPP en anglais) et adopté par l'Etat de Genève. Toutefois, le présent rapport traitant de conformité à la LIPAD, c'est l'expression de données personnelles qui sera utilisée ici, dans le sens que lui donnent cette loi ainsi que les juristes.

Données personnelles

La notion de donnée personnelle se réfère à la définition contenue dans la LIPAD (art. 4, lettre a LIPAD). Il s'agit donc d'un terme réservé, qui ne doit pas être confondu avec la notion, plus large, de donnée *confidentielle* : si toute donnée personnelle doit rester confidentielle (art. 37 LIPAD), il peut

---

[7] *Giorgio Pauletto,* L'information comme ressource stratégique dans l'administration*, présentation donnée à la journée de rencontres de l'Observatoire technologique du 18 novembre 2004, p. 14 (http://fr.slideshare.net/giorgiop5/linformation-comme-ressource-stratgique).*

exister des données qui, tout en étant jugées *confidentielles* par l'administration, ne constituent pas pour autant des données personnelles au sens de la LIPAD.

Comme il vient d'être dit, une information, n'est, *en soi*, jamais personnelle : c'est le *lien* qui peut être établi entre cette information et une personne physique ou morale (identifiée ou identifiable) – autrement dit son contexte – qui la consacre comme telle. Cette caractéristique rend particulièrement ardue la qualification de « donnée personnelle » en informatique, et donc l'examen de la conformité des pratiques de l'Etat à la LIPAD dans le cadre de l'AeL.

Confidentialité

La confidentialité est un élément de la sécurité des données. La confidentialité d'une donnée est assurée lorsque cette dernière est protégée contre tout accès indus de tiers. Comme pour tout aspect propre à la sécurité des données, la confidentialité ne peut être garantie que par la combinaison de mesures organisationnelles et de mesures techniques.

Sécurité des données

La sécurité des données vise à garantir à la fois leur confidentialité, leur intégrité, leur disponibilité (cf. art. 37, al. 2 LIPAD), leur licéité (autrement dit leur conformité au cadre réglementaire), ainsi que leur authenticité (imputabilité, non-répudiation et traçabilité).

La sécurité des données se compose de deux aspects complémentaires : la sécurité opérationnelle (les « mesures techniques » de l'art. 37, al. 1 LIPAD), d'une part; la sécurité de l'information (les « mesures organisationnelles » de l'art. 37, al. 1 LIPAD), d'autre part. La sécurité opérationnelle met en œuvre et maintient les mesures techniques de sécurité, visant à diminuer les risques liés au traitement automatisé de l'information. La sécurité de l'information, pour sa part, inclut en outre les mesures organisationnelles de protection du patrimoine informationnel, en particulier la gestion des accès.

Portail de l'Etat

L'expression « portail de l'Etat » désigne le point d'entrée unique aux prestations publiques – à savoir les services produits par un office de l'administration – et à la communication institutionnelle en ligne. Il suppose une harmonisation graphique et architecturale du site Internet de l'Etat et se révèle complémentaire des prestations en ligne en ce qu'il peut faciliter leur accès au citoyen. Il permet de présenter les informations et les prestations de l'Etat dans une logique de prestation et en fonction de thèmes, et non pas en fonction des cloisonnements de l'administration issus de son organisation interne. Il s'avère en cela le support idéal de l'administration en ligne.

Bilan des 10 prestations d'impulsion en matière de protection des données

Dérogations à la LIPAD concernées par l'article 69

Les dérogations à la LIPAD rendues possibles par l'article 69, alinéa 1 LIPAD sont au nombre de huit. Elles sont énumérées par l'article 69, alinéa 2 LIPAD :

- exigence d'une tâche légale (art. 35, al. 1 *in fine* LIPAD);
- caractère *nécessaire* du traitement pour l'accomplissement d'une tâche légale (art. 35, al. 1 et 2, art 36, al. 1, lettre a, et 41, al. 1, lettre a LIPAD) ou caractère *absolument indispensable* du traitement pour l'accomplissement d'une tâche légale (art. 35, al. 2 LIPAD);
- exigence d'un lien matériel étroit entre les tâches pour l'utilisation du NAVS13 (art. 35, al. 4, 2e phrase LIPAD);
- caractère reconnaissable de la collecte (art. 38, al. 1 LIPAD);
- preuve du traitement conforme par l'institution requérante (art. 39, al. 1 LIPAD);
- communication subséquente au responsable LIPAD (après communication entre institutions publiques) (art. 39, al. 2 LIPAD);
- obligation de consultation préalable des personnes concernées (art. 39, al. 10 LIPAD);
- destruction ou anonymisation des données obsolètes (art. 40 LIPAD).

D'emblée, il était clair que les dérogations autorisées ne représentaient pas un blanc-seing en faveur de l'administration durant la durée du programme de l'AeL, mais qu'elles devaient n'être utilisées qu'en cas de nécessité[8].

La DGSI et les services responsables des prestations d'impulsion se sont efforcés de mettre ces dernières en conformité avec la loi par diverses mesures de sécurité, ainsi que, sur le plan juridique, par l'adoption de conditions générales AeL informant les futurs utilisateurs des aspects liés à la LIPAD. L'expérience retirée de ces mises en conformité – déjà saluée par le rapport intermédiaire d'évaluation du programme AeL rendu en décembre 2013 par les préposées de l'époque – est relatée ci-après[9].

---

[8] *Ce principe a été souligné par le PPDT dans sa prise de position du 28 octobre 2011 (Bureau des préposé-es à la protection des données et à la transparence, « Mise en œuvre de l'art. 69 LIPAD selon le PPDT dans le cadre de l'Administration en ligne », http://www.ge.ch/ppdt/doc/documentations/PPDT_Prise_de_position_2011_I_013_Art_69_LIPAD_mise_en_oeuvre_selon_PPDT_V.pdf).*

[9] *PPDT, Rapport intermédiaire d'évaluation du programme AeL, décembre 2013*

Les problématiques transverses

Avant d'aborder séparément les différentes prestations d'impulsion, il convient d'aborder les problématiques récurrentes posées par la mise en service de toute prestation en ligne. En effet, si les problématiques posées par un contexte particulier à l'une ou l'autre prestation peuvent apparaître occasionnellement, les risques inhérents à la mise en œuvre des prestations en ligne sont avant tout communs.

Problématiques d'harmonisation

Afin de gérer les problématiques communes à toutes les prestations en ligne, une plate-forme unique (ci-après : socle) a été développée dans le cadre du programme AeL. Elle permet notamment de renforcer la sécurité opérationnelle des données par une gestion centralisée et cohérente des services de base, ce qui réduit en outre les difficultés de mise en œuvre de prestations en ligne supplémentaires. Les services fonctionnels de base rendus par le socle sont les suivants :

- stockage en ligne des demandes administratives et des iDossiers personnels (ou espace utilisateur);
- gestion du cycle de vie (et donc des changements d'état) des demandes en ligne, tel que défini par le métier en fonction de ses pratiques de traitement;
- contrôle des accès aux iDossiers, le contrôle des accès représentant un pan essentiel de la sécurité des données et de la garantie de leur confidentialité;
- planification des tâches de base telles que l'envoi automatique de courriers électroniques (de relance ou d'information) à l'attention des parties prenantes d'une prestation ou la mise à jour automatique de l'état d'un dossier;
- mise à disposition d'un espace d'échange permettant la collecte d'informations nécessaires à la délivrance de prestations, régulièrement synchronisé avec les systèmes accessibles par le seul personnel administratif (systèmes « *back-office* métier »);
- hébergement du système de paiement en ligne et de suivi des paiements, avec mise à jour automatique de la demande métier en fonction du résultat de la transaction de paiement.

L'existence du socle permet une sécurité accrue des données et permet d'offrir à moindre coût le développement cohérent des prestations en ligne à venir. Mais l'exigence d'harmonisation ne s'arrête pas aux seuls aspects techniques.

Problématiques d'authentification

La confidentialité requise par les prestations en ligne dépend avant tout du type de données qui sont échangées avec l'utilisateur ou qui lui sont rendues accessibles. Lorsqu'il est question de données confidentielles, *a fortiori* de données personnelles, il est nécessaire de protéger l'accès à ces données ainsi qu'aux prestations associées.

Afin de permettre aux chefs de projets des prestations d'impulsion de choisir le mode d'authentification approprié en fonction de la nature de la prestation, une typologie de trois régimes différents a été proposée : *l'absence d'authentification*, lorsqu'il n'est pas nécessaire de connaître l'identité du demandeur dès lors que le bénéficiaire de la prestation est connu et que la demande, même effectuée à son insu, ne peut pas lui porter préjudice; *l'authentification faible*, dans les rares cas où les données échangées ne sont guère confidentielles; enfin, *l'authentification forte* dans tous les autres cas. L'authentification faible implique l'utilisation d'un nom d'utilisateur et d'un mot de passe. Selon les cas, une adresse de courrier électronique valide peut être utilisée comme nom d'utilisateur. L'authentification forte, elle, s'effectue : soit à l'aide d'une clef SuisseID, soit avec un nom d'utilisateur, assorti d'un mot de passe et d'un code de connexion à usage unique transmis à chaque connexion sur le téléphone mobile de l'utilisateur.

Alors que dans un premier temps l'enregistrement aux e-démarches se faisait de manière séparée pour chacune d'entre elles, permettant de moduler le type d'authentification en fonction du contenu de la prestation proposée, depuis 2013, seul le mécanisme d'authentification forte reste disponible lors de la création du compte AeL. Le but poursuivi vise une simplification de la gestion du iDossier. C'est ainsi que la prestation « Autorisation de manifestation » (P6), initialement soumise à une authentification faible afin d'ouvrir la prestation à tous plutôt que d'assurer une sécurité accrue des transactions, a été soumise à une authentification forte.

Une autre problématique relative à la confidentialité a trait à la communication à un tiers de documents contenant des données personnelles par le jeu des accès partagés aux iDossiers. Il existe plusieurs exemples limites. Citons-en deux parmi d'autres :

– le second époux d'une femme divorcée peut-il, par le biais d'un accès partagé au iDossier de cette dernière, accéder à des documents officiels contenant des données personnelles concernant le premier époux, tels que le jugement de divorce ?

– le service en charge de délivrer une bourse à des enfants majeurs peut-il avoir accès aux données de leurs parents – condition nécessaire pour obtenir une telle aide – même lorsque ces derniers s'y opposent ?

Par ces exemples, on voit à quel point la garantie de la confidentialité peut s'avérer complexe dans le cadre des prestations en ligne.

Le premier cas peut se régler aisément : il suffit que l'accès du second époux au iDossier de sa conjointe soit le fait d'un acte exprès de cette dernière, et non d'une option par défaut. C'est du reste la solution qui est déjà en place. Dès lors que rien ni personne ne peut empêcher une femme de montrer à son second mari l'exemplaire papier de son jugement de divorce, on ne voit pas en quoi l'accès partagé qui aboutit au même résultat pourrait poser problème au regard de la LIPAD.

Le second cas s'avère plus délicat, et nécessite de recourir à la loi sur le fond. L'article 6, alinéa 3 de la loi sur les bourses et prêts d'études (C 1 20) stipule ainsi que les parents dont les données sont consultées par le service des bourses et prêts d'études doivent en être informés, sans qu'il soit *a priori* nécessaire d'obtenir leur accord.

Problématiques de vérification d'identité

Les prestations qui appellent un degré hautement confidentiel nécessitent avant tout de vérifier l'identité du demandeur de la prestation. Toutefois, une lourdeur excessive des processus d'authentification risque de décourager les citoyens d'y accéder. Elle pourrait même contrevenir à la LIPAD, celle-ci imposant de protéger les données personnelles par des mesures techniques *appropriées* (art. 37, al. 1 LIPAD) et de ne pas requérir d'une personne des données la concernant qui ne seraient pas nécessaires au but proposé (art. 36, al. 1, lettre a LIPAD). Ces prestations qui nécessitent une vérification d'identité de l'utilisateur utilisent toutes le mécanisme d'authentification forte. La vérification de l'identité de l'utilisateur peut se faire de plusieurs manières : soit par le biais d'une clef SuisseID, soit par présentation d'un document d'identité à un guichet de l'Etat désigné à cet effet, par l'envoi à l'utilisateur d'un courrier postal recommandé comportant un code d'activation, ou encore au moyen d'un formulaire complété par l'utilisateur et envoyé par voie postale à l'administration.

Afin d'éviter d'inutiles complications pour l'utilisateur, une inscription initiale unique est requise pour l'ensemble des prestations nécessitant une authentification forte. C'est ensuite à l'utilisateur qu'il revient de s'inscrire à chaque service spécifique, en fonction de ses besoins.

Problématiques de sécurité

La méthode de projets HERMES recommande l'élaboration d'un *concept SIPD* afin d'assurer la mise en place d'une politique efficace de protection des données. Ce concept a été mis en œuvre au sein de l'administration en juillet 2012 et se place dans une perspective de gestion des risques : il aide à identifier les exigences et les risques liés à la sécurité, puis à prendre les décisions de traitement des risques qui en découlent, avant de sélectionner et de mettre en œuvre des mesures appropriées afin de ramener les risques à un niveau acceptable.

Un point particulier mérite d'être souligné : celui de la limitation des copies de données. La sécurité des données personnelles – notamment leur intégrité et leur authenticité – nécessite d'éviter la présence de copies en production dans différents services. Il est donc nécessaire à la fois d'empêcher autant que possible la création de copies à des fins autres que de sauvegarde et d'encadrer correctement la gestion des fichiers de référence.

Concernant le premier point, la mesure est déjà appliquée : il s'agit de privilégier les accès à distance aux données personnelles plutôt que leur mise à disposition sous forme de copie. La réponse au second point consiste à établir la liste des fichiers intéressant plusieurs services et de désigner officiellement pour chacun d'eux celui qui sera chargé de le gérer et de le mettre disposition des autres services en application des conventions de transmission de données qu'il aura passées avec eux. Cette procédure est en cours d'étude.

Problématiques liées à l'exploitation de solutions externes

Certaines problématiques peuvent naître de l'intégration dans la prestation en ligne d'une application externe, qui menace la cohérence technique mise en place par le socle, en particulier si l'on considère la nécessaire évolution des prestations dans le temps. Toute modification doit alors s'assurer dès la conception du maintien de la cohérence de l'architecture de l'application ainsi modifiée avec le socle[10]. C'est le cas des prestations qui incluent un volet permettant le paiement électronique des émoluments, mais aussi des outils documentaires externes, comme la prestation « Espace école en ligne » (P10), l'illustre[11].

[10] *En d'autres termes, il s'agit d'assurer la compatibilité ascendante depuis le socle.*

[11] *Voir ci-dessous « P10. Espace école en ligne », p. 21s.*

Problématiques d'encadrement des projets

La mise en œuvre d'une prestation en ligne doit être considérée comme un projet informatique à part entière. Les aspects problématiques propres à la prestation ne sont en effet souvent mesurés qu'après sa conception technique, en particulier à l'occasion du déploiement, voire à l'occasion du développement de nouvelles prestations par « clonage » de prestations similaires préexistantes. Cela suppose un encadrement adéquat tout au long de la réalisation du projet et jusqu'à sa mise en service, ainsi qu'un arbitrage entre les différents besoins exprimés.

Pour assurer un tel encadrement et une évolution cohérente entre les prestations tenant compte de l'ensemble des aspects techniques, métier et légaux (en particulier la conformité à la LIPAD), le programme AeL bénéficiait d'un comité de pilotage *ad hoc*, à même d'arbitrer les priorités, d'anticiper les problématiques et d'éviter les blocages.

Problématiques de visibilité

L'objectif principal de l'AeL et des e-démarches est de rendre les tâches administratives plus simples et de répondre aux attentes des usagers, en particulier par des gains de temps sous forme :

- d'une aide dans la rédaction même de la démarche (ex. : demande de modification d'acompte, remplissage de la déclaration d'impôts);
- d'une accélération de la vitesse de traitement des demandes (ex. : Facture Express, une des neuf prestations complémentaires);
- d'une suppression des déplacements (ex. : e-paiement);
- d'une diminution des échanges de courrier papier (ex. : i-correspondance);
- d'une suppression des contraintes horaires des guichets (accès aux services 24 heures sur 24 et 7 jours sur 7);
- de l'accès à l'état d'avancement d'un dossier par le demandeur (disponible pour une grande partie des prestations en ligne);
- de l'amélioration de la qualité du service et de l'information (ex. : iDossier)[12].

Le premier des facteurs permettant un accès plus aisé aux e-démarches est leur facilité d'utilisation, d'où le souci d'harmoniser l'ergonomie de l'ensemble : la difficulté d'apprentissage de l'administré s'en trouvera diminuée d'autant, et l'encouragera, une fois familier avec une prestation, à en utiliser d'autres. Des normes d'ergonomie cohérentes à l'ensemble des

[12] *PL Bouclement 10177, op. cit, pp. 14 s.*

e-démarches ont ainsi été mises en place. Ces normes ergonomiques seront prises en compte pour l'élaboration d'une nouvelle plateforme Internet de l'Etat de Genève.

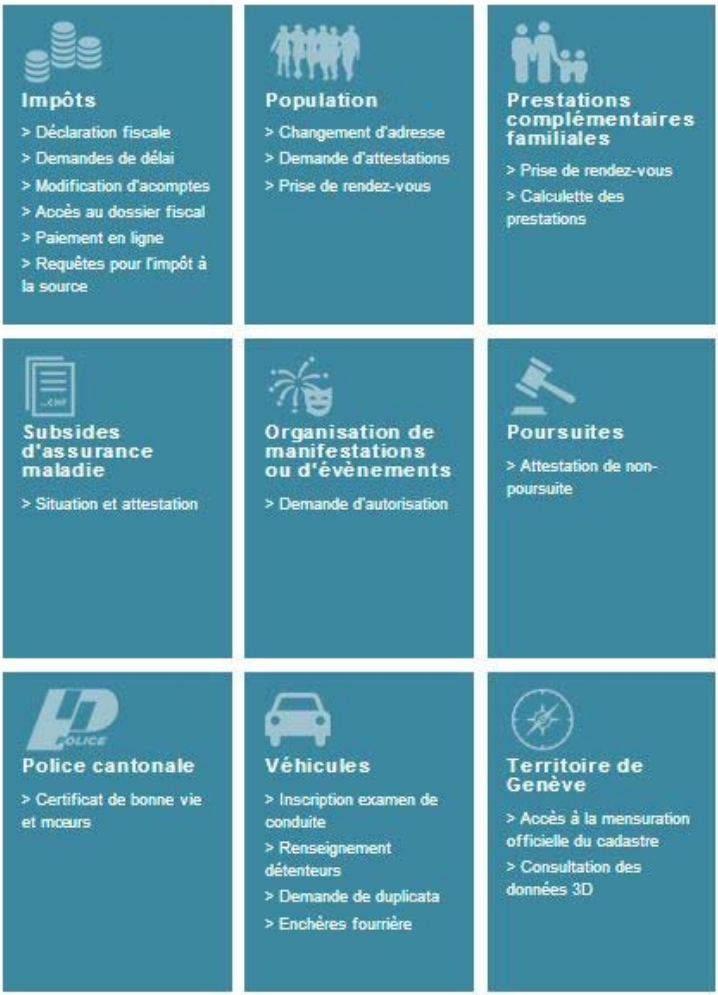
Le second facteur tient à la facilité de l'inscription elle-même. Le respect de la LIPAD implique, comme on l'a vu, une certaine contrainte pour s'assurer d'un degré suffisant d'authentification. Toutefois, des efforts ont été menés pour rendre l'inscription plus aisée. Ainsi, pour faciliter l'accès et l'utilisation des prestations, un centre d'assistance avec un seul numéro d'accès (0 840 235 235) est ouvert du lundi au vendredi de 8h à 18h. Ces deux dernières années, ce centre d'assistance a également été ouvert le week-end pendant la deuxième quinzaine de mars. Il s'agissait de répondre aux attentes des contribuables qui remplissent leurs déclarations d'impôt. De même, pour raccourcir le délai d'inscription aux e-démarches (de l'ordre de 3 jours, compte tenu de l'envoi d'un courrier recommandé), des guichets d'inscription ont été ouverts à l'AFC et à l'OCPM. A ces guichets, le citoyen peut recevoir immédiatement ses codes d'accès après vérification de son identité.

Enfin, le dernier facteur essentiel tient à la visibilité même des e-démarches sur le site officiel de l'Etat : une prestation en soi utile à l'administré mais dont il ignore l'existence ou dont il ne sait pas comment y accéder, ne lui sera d'aucune utilité.

Chaque e-démarche constitue déjà en elle-même un point d'entrée unique dans l'administration pour l'utilisateur. Elle engendre une organisation des services selon les besoins des citoyens et non pas en fonction des structures de l'administration, ce qui là encore occasionne un gain de temps.

Une étude sur la visibilité des e-démarches au sein du site de l'Etat de Genève a permis d'améliorer leur accès par une signalisation claire, à l'aide notamment d'un logo spécifique, et par une page d'accueil des e-démarches qui présente l'ensemble de celles disponibles à un large public[13] :

[13] *La reproduction ci-après ne mentionne toutefois pas les prestations concernant les subventions énergie.*



Cette présentation ne pouvait être réalisée avant la mise en service d'un nombre suffisant de prestations en ligne.

A l'heure actuelle, des dizaines de milliers de particuliers et près de 10 000 entreprises sont inscrits aux e-démarches.

Les efforts de visibilité fournis ne manqueront pas d'accroître le nombre des inscriptions aux e-démarches.

Les dix prestations d'impulsion prioritaires

Dans le but de mettre en œuvre une AeL aussi efficiente qu'attractive, le Conseil d'Etat a pris le parti de développer dix prestations d'impulsion, avec pour but d'inciter leurs usagers à les utiliser, puis à y faire appel de manière régulière[14].

L'examen des problématiques spécifiques rencontrées dans la mise en œuvre de chacune des dix prestations d'impulsion vient compléter l'exposé des difficultés transverses susmentionné. Pour chaque prestation d'impulsion, un bref descriptif de la prestation[15] est suivi des points qu'il a fallu résoudre pour la rendre compatible avec les exigences de la LIPAD.

P1. Impôts personnes physiques

Cette prestation offre au contribuable la possibilité d'interagir directement avec l'administration fiscale, en particulier pour envoyer sa déclaration, transmettre des documents, demander des *duplicata* ou des attestations, consulter les documents relatifs aux exercices passés : avis de taxation, bordereaux, décisions en matière de répartition intercantonale ou encore relevés de compte. Le contribuable peut également consulter et imprimer des documents tels que les relevés d'intérêt, les relevés d'arrangement; il peut enfin recevoir ses factures dématérialisées de l'administration fiscale, par le biais de son fournisseur « e-banking ».

En matière de protection des données, cette prestation présente un risque élevé, puisque l'AFC est appelée à communiquer au contribuable l'ensemble des échanges passés avec l'administration, y compris les déclarations fiscales des exercices antérieurs. Pour assurer une plus grande sécurité, l'espace de données des métiers n'a été rendu accessible qu'aux contribuables inscrits à ce service, bien distinct du simple téléversement de la déclaration.

P2. Impôts à la source

Cette prestation facilite grandement la gestion de l'impôt à la source pour les personnes morales. Ces dernières peuvent, grâce à elle, remplir ou établir les attestations par téléchargement, annoncer l'arrivée d'un employé imposé à la source, remplir des formulaires, ou encore annoncer un changement de situation.

La mise en œuvre de cette prestation a suscité des difficultés pour authentifier le titulaire (employeur personne morale ou personne physique

14 *PL AeL (PL 10177), op. cit., p. 14*

15 *Pour une description plus précise de chacune des dix prestations d'impulsion, il est renvoyé au PL bouclement 10177, op. cit., pp. 3 ss*

indépendante) et ses représentants, les registres officiels existants couvrant des populations disjointes. Il est donc difficile de valider l'identité des titulaires de compte AeL susceptibles d'être soumis à l'impôt à la source pour leurs employés. Il a été décidé de proposer plusieurs référentiels (numéro ZEFIX, RC cantonal ou REG), et de permettre à l'employeur d'en fournir au moins un. Il est envisagé de compléter l'ensemble avec le numéro IDE, le nouvel identifiant des entreprises introduit par la Confédération, qui permettra notamment d'identifier les entreprises qui se font représenter dans l'AeL par des mandants professionnels. Ces difficultés ne justifient toutefois pas une modification de la LIPAD.

P3. Portail social

En visant les objectifs du portail social décrits dans l'exposé des motifs, les e-démarches suivantes ont été mises en service :

– la prise de rendez-vous pour le service des prestations complémentaires (SPC) : les bénéficiaires potentiels de prestations complémentaires familiales (PCFam) peuvent prendre rendez-vous en ligne avec le service chargé de la prestation;
– la calculette du SPC : elle permet aux bénéficiaires potentiels de PCFam d'évaluer les montants qu'ils pourraient recevoir;
– la calculette du service de l'assurance maladie (SAM) : cet outil permet de vérifier le droit à un subside d'assurance-maladie et, le cas échéant, de remplir un formulaire de demande en ligne;
– la possibilité d'accès en ligne à son relevé de subsides d'assurance-maladie, ce qui permet au citoyen de vérifier sa situation et celle de sa famille.

Enfin, l'attestation RDU sera également mise en ligne dans le cadre de la mise en œuvre du SI RDU (Système d'information du RDU).

L'iDossier social utilisera la même architecture que l'iDossier fiscal, afin d'assurer une cohérence dans les dispositifs de sécurité et juridique. Les risques et les mesures de sécurité évoqués à propos de la P1 s'appliqueront donc de la même manière à la P3.

P4. Portail de la population

Le portail de la population offre des prestations aux citoyens, ainsi qu'à certaines catégories socioprofessionnelles, notamment :

– l'annonce d'un changement d'adresse;
– la commande d'attestation : l'usager peut demander différentes attestations en ligne, telles que l'attestation de résidence, l'attestation de départ, etc. Pour améliorer encore la qualité de ses services, l'OCPM attend toutefois

que la signature électronique soit reconnue, tant au niveau légal que pour des motifs de sécurité, pour déployer une solution totalement automatisée qui accélérera le processus de délivrance de la prestation. Pour l'heure, l'acheminement de l'attestation reste manuel, en raison du tampon officiel qui doit être apposé sur le document;

– la modification des rendez-vous pour la prise des données biométriques nécessaires à la confection des titres de séjour pour les étrangers : l'usager qui dispose d'une convocation a la possibilité de modifier son rendez-vous en ligne, sauf dans les cas d'avis de fin de validité pour lesquels une évolution de cette prestation est prévue;
– la fonction « Mes données personnelles OCPM » qui offre la possibilité de consulter ses données personnelles en ligne et de soumettre des demandes;
– les régies ont la possibilité de communiquer en ligne les changements d'adresse, sans pour autant bénéficier d'un accès à la base de données de la population.

Une mention spéciale doit être faite à propos du module permettant l'annonce de changement d'adresse par l'administré lui-même. Il s'agit en effet d'un module externe du nom de Gestar, développé par une entreprise privée. Gestar a été choisi parce que son utilisation par d'autres cantons offrait le gage d'une maturité suffisante de la solution. Dès lors qu'il s'agit d'un programme externe, le contrôle du flux des donnés est pris en charge par un autre progiciel que le socle propriétaire de l'AeL; il s'ensuit la nécessité de vérifier à l'avenir, tout au long de son évolution, sa conformité aux règles de protection des données implémentées dans l'architecture technique de l'AeL. On notera en outre que l'OCPM s'attend à ce que le nombre d'inscriptions à ses prestations augmente dès lors que la prestation relative à l'annonce de changement d'adresse sera gratuite si elle est faite en ligne.

P5. Direction générale des véhicules

Les prestations en ligne proposées par la direction générale des véhicules ont été étendues en matière de facturation et de paiement en ligne ou de démarches administratives, telles que les demandes de renseignements sur le détenteur d'une immatriculation ou les demandes de duplicata de permis échus.

On notera que la possibilité d'obtenir automatiquement par SMS des informations sur le détenteur d'une plaque d'immatriculation, pourtant conforme à l'article 125, alinéa 3, de l'ordonnance sur l'admission des personnes et des véhicules à la circulation routière (OAC) a été revue puisqu'elle était susceptible de profiter aux bandes organisées en matière de

cambriolage. Désormais, tout particulier doit le faire en ligne et le tarif de cette prestation a été revu à la hausse. Les informations ne sont transmises au demandeur qu'après analyse des motifs de sa requête, ceci afin d'éviter les demandes de simples curieux. Là encore, la solution trouvée pour rendre possible cette e-démarche ne nécessite pas la modification de cette dernière.

Dans ce cadre, les prestations en ligne profitent non seulement aux citoyens, mais également à l'administration, puisqu'elles permettent d'échanger par voie électronique des informations avec d'autres services, notamment pour les rapports de police, de contraventions, de réquisitions de poursuite, ou encore certains dossiers de la chambre administrative de la Cour de justice. Ces transferts sont tous couverts par une base légale formelle, si bien qu'aucune modification légale n'est requise.

P6. Autorisation de manifestation

Cette prestation permet à quiconque de déposer une demande d'autorisation de manifestation avec la possibilité de modifier, compléter ou supprimer sa demande en ligne. L'organisateur peut accéder aux informations pour le suivi et l'historique de sa demande, payer en ligne et imprimer lui-même l'autorisation.

P7. PME Genève

Il s'agit d'une plateforme d'information et de gestion des procédures administratives à l'intention des entreprises qui rapproche les entreprises de l'administration en simplifiant l'interactivité des procédures.

Les entreprises peuvent directement enregistrer les modifications (RC, AVS, TVA, SUVA, statistiques, etc.) qui les concernent (en phase avec la stratégie nationale de la Confédération) et accéder aux informations et aux formulaires nécessaires à leur activité, notamment dans les domaines juridique, d'assurances sociales, de permis de travail, de fiscalité, ou d'aides financières. En outre, la plateforme permet de s'informer sur les pré-requis juridiques pour exercer une profession réglementée dans le canton de Genève (40 professions sont concernées, telles que : médecins, pharmaciens, ramoneurs, restaurateurs, hôteliers, aides-dentiste, courtiers en assurances) et l'utilisateur pourra remplir en ligne les formulaires nécessaires.

Cette prestation est accessible sans authentification préalable, car le bénéficiaire est connu de l'administration. La prestation couvre la faculté de payer en ligne, ce qui implique la nécessité d'intégrer les aspects de sécurité habituels pour authentifier le payeur et garantir la confidentialité du processus.

La P7 étant par vocation ouverte aux PME, elle pose également la question du référentiel des personnes morales évoqué ci-dessus (cf. P2).

P8. Plan d'affectation du sol et autorisations de construire

En collaboration avec la Fédération des architectes et ingénieurs de Genève (FAI), un guichet des autorisations de construire a été développé en utilisant des formulaires en ligne comportant des fonctions géomatiques et faisant appel aux données du SITG. Durant l'année 2012, le guichet a été mis à disposition de quelques architectes à titre d'essai. Toutefois, ce guichet en ligne n'a pu être ouvert à un plus large public, car l'architecture technique n'était pas suffisamment fiable et surtout parce qu'il ne visait que le dépôt des demandes d'autorisation de construire et pas le traitement administratif des dossiers. Faute d'une dématérialisation de bout en bout, il rendait la prestation plus coûteuse, au lieu de la simplifier.

Dans le cadre de la réforme des autorisations de construire, notamment de l'accélération de la délivrance de l'autorisation de construire par procédure accélérée (APA), une solution utilisée dans plusieurs cantons et soutenue par la Confédération (CAMAC) a été identifiée pour le traitement administratif susmentionné. Une étude est conduite en vue d'adapter cette solution au nouveau processus APA, dont le succès se confirme. Ces travaux s'inscrivent également dans la ligne souhaitée par le Grand Conseil par le biais de la motion 2079. Certains éléments du guichet susmentionné pourront être réutilisés.

Comme pour la P7, cette prestation était accessible sans authentification préalable, car le bénéficiaire est connu de l'administration; en d'autres termes, c'est le bénéficiaire annoncé qui se verra proposer la prestation, si bien qu'il pourra toujours ne pas y donner suite si elle a été requise par un tiers pour lui à son insu.

P9. Gestion administrative des praticiens

La prestation permet à quelque 20 000 médecins, pharmaciens, droguistes et laborantins de soumettre une demande de droit de pratique ou d'autorisation d'exploiter. Elle informe également les internautes sur les types et la localisation des différents praticiens.

La prestation couvre en outre la faculté de payer en ligne, ce qui emporte la nécessité d'intégrer les aspects de sécurité habituels dans le domaine de l'e-paiement pour authentifier le payeur et garantir la confidentialité du processus.

P10. Espace école en ligne

Le projet Espace école en ligne constitue un des points forts du plan directeur « Enseigner et apprendre à l'ère numérique » et offre une grande ouverture sur la société de l'information. Basé sur des standards ouverts, il renforce les liens avec les partenaires pédagogiques, favorise l'intégration

rapide des technologies numériques et des pratiques. La plateforme est directement utilisable depuis une salle de cours dotée d'équipements numériques.

La solution fournit un référentiel d'identité tant pour les élèves et les enseignants ainsi que leurs groupes pédagogiques (établissement, classe, cours, disciplines). Avec cette identité numérique, chaque enseignant et élève bénéficie d'un accès personnalisé. Cette plateforme permet également de partager du contenu sur les services disponibles pour la pédagogie :

– cours en ligne,
– espace numérique de travail,
– site de disciplines en conformité avec HarmoS,
– ressources pédagogiques et manuels d'enseignement numériques,
– site d'établissement,
– blog.

Cette industrialisation permet la gestion d'annuaires assurant une authentification correcte des acteurs – enseignants et élèves – accédant à ces espaces. Toutes les technologies mises en place (liées à l'environnement partagé) étant extérieures au socle, se pose un problème particulier de sécurité des données personnelles. Le contrôle des flux assuré par le socle AeL est ainsi limité à la seule fonction d'authentification. Le reste du flux est pris en charge par l'espace collaboratif mis en œuvre.

Sur le plan juridique, il faut s'assurer que le prestataire externe de l'espace collaboratif mis en œuvre est soumis à des normes légales de protection des données similaires à la LIPAD, en particulier concernant la suppression des données personnelles par le prestataire externe lorsque celles-ci ne sont plus utiles. Cet annuaire génère pour les élèves des identifiants sous forme de pseudonyme, permettant ainsi des activités pédagogiques avec des services Web dont l'hébergement en Suisse ne peut être garanti.

Avec la P10, le DIP met en place non pas une simple prestation, mais plutôt un mécanisme, beaucoup plus complexe, d'industrialisation de prestations en ligne. L'outil choisi par l'enseignant conditionne donc la qualité de la sécurité des données personnelles, ce qui en fait la prestation d'impulsion la plus délicate à traiter. Ce risque est balancé par l'accompagnement de l'élève par l'enseignant dans l'usage et l'expérience du monde numérique qu'il va développer sous l'égide de l'enseignant.

Cadre réglementaire et principes reconnus

Pour juger de la conformité des prestations en ligne à la LIPAD, il est impératif de tenir compte du cadre légal applicable en complément de cette dernière et des normes et bonnes pratiques internationales en vigueur.

Cadre légal

En matière de protection des données personnelles, plusieurs textes législatifs entrent en compte dans le cadre d'une mise en conformité des prestations en ligne à la LIPAD. Il s'agit des textes suivants :

- LIPAD (rs/GE A 2 08);
- RIPAD (rs/GE A 2 08.01);
- LPD, dans la mesure où l'administration cantonale est appelée à effectuer des prestations pour le compte de la Confédération et où elle s'applique à l'ensemble des personnes morales et physique, autrement dit aux utilisateurs de l'AeL;
- ROGSIC (rs/GE B 4 23.03), qui décrit le partage des responsabilités entre la DGSI et les maîtres de fichiers;
- normes légales applicables aux métiers de l'administration, telles que le secret de fonction, le secret fiscal genevois (art. 11 LPFisc), ainsi que les dispositions justifiant du besoin de données personnelles pour la mission d'un service administratif ainsi que du transfert de ces données d'un service à l'autre. Ces normes légales peuvent justifier les pratiques métier prises en compte par les prestations en ligne, voire induire la qualification des données traitées par un service; ainsi, les dispositions relatives au secret fiscal déterminent-elles que toute donnée traitée par l'AFC doit, de ce fait même, être considérée comme confidentielle, quand bien même il ne s'agirait pas de données personnelles au sens de la LIPAD.
- directives transverses de l'Etat relatives à cette problématique : directive relative à la classification des informations (EGE-10-12), directive relative au partage d'informations (EGE-09-02), directive sur les ressources matérielles et immatérielles TIC (EGE-10-15), Politique de sécurité de l'information (PSI), etc.;
- loi sur l'archivage des données (LArch – rs/GE B 2 15), qui fait pendant à l'obligation faite par la LIPAD de supprimer les données inutiles ou obsolètes.

Les normes, standards et bonnes pratiques

ISO 27 000, PPRP, PMM

Pour appliquer ces dispositions légales, l'Etat de Genève s'appuie sur un ensemble de bonnes pratiques internationalement reconnues dans le domaine de la sécurité de l'information : le cadre normatif ISO / IEC 27000, les principes généralement reconnus en matière de protection des renseignements personnels (PPRP, en anglais GAPP), ainsi que le modèle d'évolution des pratiques en matière de protection des renseignements personnels (Privacy Maturity Model – PMM). Le modèle PMM permet aux entités de se faire une bonne idée de leur situation et, au fil des examens, de leurs progrès. C'est pour sa capacité à traiter la protection des données personnelles dans toute sa complexité, en fonction des exigences fixées par la loi mais aussi en tenant compte des impératifs concrets de mise en œuvre de ses principes, qu'il a été préconisé d'implémenter PMM dans l'indicateur de conformité à la LIPAD dont vient de se doter l'AFC.

HERMES

Il s'agit de la méthodologie officielle de la Confédération, devenue depuis aussi celle de l'Etat de Genève. Cette méthode relative à la gestion des projets informatiques inclut parmi ses exigences l'expression de la sûreté de l'information et de la protection des données (SIPD). Cette approche permet notamment une prise en compte *dès la conception* d'un projet les aspects légaux relatifs au traitement de l'information (« *Privacy by design* »). La protection des données est ainsi prise en compte très en amont dans le cycle de vie du projet, ce qui permet en particulier de gérer en temps utile les questions relatives à la gestion des accès et, plus généralement, à la protection des données, préoccupations qui pourraient s'avérer beaucoup plus coûteuses si elles étaient abordées plus tard. L'usage de cette méthode assure en outre un traitement homogène de l'ensemble des projets sur cette problématique. De plus, la DGSI a développé, conformément aux modèles de la Confédération, des outils permettant l'évaluation de ces exigences.

Diagnostic et retour d'expérience

Un changement de paradigme, trois acteurs principaux

Les obligations juridiques qui découlent pour l'administration des e-démarches n'ont pas toujours été évaluées de la même manière par tous les acteurs. Alors que, de manière classique, l'intégralité de la prestation est remplie par le métier, avec les prestations en ligne, c'est le système d'information (aspects *techniques* comme aspects *processuels*) qui entre en interaction directe avec le citoyen. Cela entraîne un partage de la

responsabilité des prestations entre le métier et la DGSI. La DGSI ne peut donc plus œuvrer en « *back office* » ou en simple exécutant technique, mais doit véritablement prendre une part active et concertée avec le métier dans la délivrance des prestations, au moyen d'une organisation transverse qui reste à parfaire. Cela revient à dire que si les métiers restent bien responsables de la délivrance de leurs propres prestations, la DGSI offre désormais une prestation visible pour l'utilisateur, essentiellement sous forme de gestion de la plateforme AeL et de continuité du service.

Du côté du citoyen, les services ne lui sont plus proposés en fonction de l'organisation interne de l'administration, mais de la logique de ses préoccupations, et sont donc classés par thèmes. C'est le rôle du portail de l'Etat que de concrétiser ce changement d'orientation. Par ricochet, cela ne manquera pas d'avoir des répercussions sur la manière dont l'administration est appelée à travailler, notamment quant à la collaboration entre les différents offices. Ceux-ci sont appelés à renforcer leur complémentarité et à se positionner en fonction de la plus-value qu'ils peuvent apporter à ces prestations en ligne, et non plus en fonction de leur seule compartimentation administrative.

Ne pas percevoir ce changement de paradigme reviendrait à laisser la gestion de l'outil informatique aux seuls techniciens ou à permettre aux métiers de réaliser leur informatique à l'insu de la DGSI ou des attentes citoyennes, entraînant des risques forts de non-cohérence entre les métiers, d'interruptions de service intempestives et de non-respect des exigences en matière de protection des données personnelles, avec les conséquences en termes d'image et de responsabilité y associées. Cela n'est pas acceptable pour le développement des prestations en ligne, et, plus généralement, des systèmes d'information. L'Etat doit se doter d'une véritable politique du numérique : d'un régime d'impulsion et d'exception qui a prévalu jusqu'ici, il convient d'adopter de nouveaux principes généraux applicables à l'ensemble des départements, principes qu'ils pourront s'approprier et intégrer à leur pratique métier.

La mise en œuvre d'une prestation en ligne engage donc trois acteurs principaux : le demandeur, ou bénéficiaire de la prestation; le service chargé de délivrer la prestation; la DGSI enfin, chargée de la cohérence fonctionnelle et technique dans la gestion des systèmes d'information. La meilleure manière de s'assurer de la conformité des pratiques de l'AeL à la LIPAD est de concevoir une approche qui tienne compte des nouveaux rôles que chacun de ces trois acteurs est appelé à jouer et qui clarifie leurs rapports.

Absence de violation de la LIPAD par l'AeL

Les initiatives prises dans le cadre de l'AeL pour assurer l'application de la LIPAD[16] montrent qu'il n'est en principe pas nécessaire d'admettre une dérogation à ses principes fondamentaux pour permettre la poursuite de l'exploitation des prestations en ligne. Tant le rapport de l'actuel PPDT rendu en décembre 2014 que le rapport intermédiaire de décembre 2013 rendu par l'ancienne préposée admet que la LIPAD a été respectée par l'AeL[17]. Les expériences menées au sein de l'AeL montrent donc qu'il est possible de concevoir des prestations en ligne dans le respect des principes actuels de la LIPAD.

En traitant l'AeL comme une exception, l'article 69 LIPAD a instauré une tolérance à d'éventuelles non-conformités de la LIPAD. Si cette mesure pouvait se justifier dans une phase transitoire, elle semble exclue pour le long terme et contredirait l'esprit même de cette loi ou constituerait un aveu flagrant d'inadaptation de l'administration aux valeurs qu'elle défend. Certes, les facilités toujours plus grandes offertes par les TIC peuvent, par le confort d'accès, de traitement et de diffusion des données qu'elles offrent, menacer la confidentialité exigée par la LIPAD en faveur de leurs titulaires.[18] Il importe donc de se montrer particulièrement vigilant et de s'organiser en conséquence plutôt que de s'octroyer d'hasardeuses licences, qui à la fois contreviendraient aux principes dignes de protection défendus par la LIPAD, risqueraient de ruiner la confiance des administrés envers l'AeL et pourraient même menacer la poursuite des échanges de données personnelles entre l'administration genevoise et les autorités publiques du reste du monde. En effet, de tels échanges sont partout soumis au *principe de réciprocité*, c'est-à-dire à la garantie offerte par l'entité requérante de ce qu'elle est soumise à des exigences légales assurant un niveau de protection des données personnelles équivalant à celui offert par la loi applicable à l'autorité requise[19].

Cela ne signifie pas pour autant que rien ne doive être entrepris pour assurer *le contrôle et la garantie de la conformité* des prestations en ligne à la LIPAD, autrement dit pour gérer les risques liés à une non-conformité à la

---

[16] *Voir ci-dessus, « Problématiques de visibilité », pp. 2 ss.*

[17] *PPDT, Rapport intermédiaire d'évaluation du programme AeL, op. cit.*

[18] *Voir notamment à ce propos la description synthétique de la norme ISO 22307 du 03 juin 2008 destinée à protéger la confidentialité des données financières dans les systèmes informatiques (http://www.iso.org/iso/fr/news.htm?refid=Ref1133).*

[19] *Voir par exemple art. 39 al. 4 lettre a et art. 39 al. 6 let. a LIPAD.*

LIPAD. Les exigences de la LIPAD induisent en effet des risques qu'il s'agit de traiter avec toute l'attention requise.

Gestion des risques, solutions préconisées

Les lignes qui suivent exposent les solutions déjà mises en œuvre ou en cours d'implantation au sein de l'administration genevoise, sans qu'il soit nécessaire à l'avenir d'envisager une modification ou une dilution des principes soutenant la LIPAD. Ces solutions permettent de couvrir les huit risques énoncés au début du présent rapport[20] et évalués par le PPDT dans son rapport intermédiaire[21].

Mise en place d'un contrôle de la conformité

Les e-démarches engagent directement les valeurs défendues par la protection des données personnelles, même si les périmètres des prestations en ligne et de la LIPAD ne se recouvrent qu'en partie. Elles nécessitent notamment que l'Etat puisse rendre compte à leurs titulaires de la sécurité des dossiers électroniques (« iDossier », ou « espace utilisateur ») et des documents qu'ils contiennent, tant sur l'aspect métier (modification et suppression de données personnelles sur demande des intéressés, contrôle du flux des données au sein de l'administration) que technique (sécurité contre les accès indus de tiers). Les prestations en ligne supposent alors une véritable *gestion de la conformité* de ces prestations à la LIPAD, et non de simples validations ponctuelles à l'occasion de leur mise en service ou sur demande des services concernés, comme cela a été le cas jusqu'à présent.

Mise en place d'un indicateur de conformité

La première mesure à prendre pour qui veut pouvoir garantir une conformité à la loi est de se doter d'une mesure du niveau de maturité atteint et des progrès accomplis en vue de diminuer les éventuels écarts constatés avec le but poursuivi. Or il n'existe à ce jour aucun indicateur de conformité permettant de savoir si et dans quelle mesure la LIPAD est respectée par l'administration genevoise, en particulier dans le cadre de la collecte et du traitement transparent des données personnelles. Cette absence de visibilité ne sera plus tolérable dès l'abrogation de l'article 69 LIPAD, quand bien même il s'avère qu'aucune violation effective des grands principes de la loi n'a été commise par l'administration. C'est ce qui a été mis en place ces derniers mois au sein de l'AFC avec le projet TICIA (« *Tax Information Confidentiality Impact Assessment* »).

---

[20] *Voir ci-dessus, « Dérogations à la LIPAD concernées par l'article 69 », pp. 8 s.*

[21] *PPDT, Rapport intermédiaire d'évaluation du programme AeL, op. cit., p. 19.*

Pour ce faire, c'est le modèle PMM, explicité ci-dessus, qui a été appliqué à l'évaluation de l'impact de la confidentialité des données fiscales dans l'organisation métier de l'AFC. TICIA a permis une identification du niveau de maturité des initiatives mises en place jusqu'à présent au sein de l'AFC et de préconiser quelques mesures concrètes et adaptées d'amélioration. Compte tenu de l'approche préconisée par PMM, le but poursuivi (la conformité à la LIPAD et le respect de la confidentialité exigée par le secret fiscal) a été établi sur la base d'une analyse des risques. Il est envisagé d'appliquer à l'avenir cet indice à tous les systèmes d'information de l'Etat, sous le nom de ICIA (« *Information Confidentiality Impact Assessment* »).

Comme indiqué précédemment, les pratiques des organisations diffèrent en matière de protection des renseignements personnels, que ce soit en fonction des lois qui leur sont applicables, de la politique interne qu'elles se donnent ou de l'état d'avancement des initiatives de l'organisation. C'est particulièrement le cas de l'AFC, dont le secret fiscal tel défini par l'article 11 de la loi de procédure fiscale (rs/GE D 3 17 – LPFisc) étend le secret à *toute donnée* traitée par elle, qu'il s'agisse ou non de données personnelles. C'est ainsi que la création d'un indice de conformité doit pouvoir s'appuyer sur une classification préalable adéquate et cohérente des données sous gestion tenant compte des exigences tant légales que métier. Cette classification est rendue possible de manière commune à l'ensemble de l'administration grâce à la directive transversale relative à la classification des informations (EGE-10-12). Cette directive offre un cadre générique pour tenir compte de l'ensemble des conditions qui influent sur la qualification des données traitées, ainsi que sur les mesures organisationnelles et techniques de protection qui en découlent. Tant cette classification des données que les mesures de protection qui y sont liées sont en cours d'exécution, notamment à l'AFC et à la DGSI.

Mise en œuvre d'un SGPD

La conformité à la LIPAD (et non plus seulement le *contrôle* de cette conformité) nécessite la mise en place d'un système de gestion de la protection des données (SGPD). Il s'agit d'un système permettant notamment de mettre en lumière d'éventuelles non-conformités et d'apporter les correctifs nécessaires. L'adoption d'un SGPD permettra de mieux positionner les priorités, et d'embrasser une vision plus vaste à partir d'une *analyse de la conformité* intégrant (et ne se limitant pas à) l'analyse des risques propres à la sécurité de l'information. C'est le but d'un SGPD que d'en permettre la réalisation.

Le SGPD qui est en cours de réalisation au sein de l'administration genevoise inclut l'indice ICIA, mais ne s'y limite pas. La LIPAD exige en

outre qu'une disposition légale justifie la transmission de données au sein de l'administration (« tâche légale », art. 35, al. 1 *in fine* LIPAD). Ce point suppose le contrôle de l'existence d'une telle disposition pour chaque transfert de données, en particulier pour chaque flux récurrent. Il correspond à l'application du *principe de finalité*, qui ne se trouve pris en compte par la LIPAD que de manière implicite.

Si cette justification des transferts de données a été respectée pour chacune des prestations mises en production par l'AeL, il s'avère nécessaire à l'avenir de rassembler les bases légales justifiant chaque transfert de données d'un service à l'autre de l'administration cantonale, dès lors que cette exigence ne s'impose pas seulement en cas de transmission à un tiers. Cette vérification est celle qui nécessite le plus important effort d'organisation au sein de l'administration.

Une piste envisagée consiste à ajouter une « couche » d'information spécifique aux données au sein de la cartographie des systèmes d'information de l'Etat, dont la stratégie est actuellement en cours de révision. Afin d'alimenter cette couche, et pour éviter les doublons dans les saisies, il pourrait être profitable de s'entendre avec le PPDT sur la réorganisation de son catalogue des fichiers « Catfich »[22], afin que les déclarations qu'il rassemble puissent permettre la mise à jour automatique de la cartographie des systèmes d'information tenue par la DGSI.

Dans les cas les plus complexes ou les plus critiques, les transferts récurrents de données conduisent à l'adoption de conventions de transmission de données entre les services concernés[23]. Elles complètent l'ensemble des mesures prises et permettent de préciser la responsabilité endossée par chacun des acteurs. De telles conventions ont déjà été mises en place, sur la base d'un modèle générique personnalisable en fonction des circonstances et des solutions techniques retenues[24], afin de garantir une cohérence dans les pratiques.

Elaboration d'un code de bonne pratique pour le SGPD

L'application de la LIPAD ne relevant pas de la seule technique, mais aussi d'une organisation permettant une gestion correcte des accès aux données personnelles par les personnes qui en sont responsables, cette loi doit

---

22 *Catalogue des fichiers, dont la tenue est exigée par l'art. 43 LIPAD.*

23 *Ces conventions correspondent aux « clauses contractuelles appropriées » de l'art. 37, al. 2 LIPAD.*

24 *En particulier la convention passée dans le cadre de la mise en œuvre de la LRDU.*

être mise à portée des personnes appelées à l'appliquer, que ce soit dans le domaine informatique ou au sein des services offrant des prestations en ligne.

Pour ce faire, un *code de bonne pratique pour le système de gestion de la protection des données* a été rédigé en collaboration avec le PPDT dans l'esprit pédagogique d'un « mode d'emploi ». Il reprend, pour les adapter au contexte genevois, les *directives sur les exigences minimales qu'un système de gestion de la protection des données doit remplir (Directives sur la certification de l'organisation et de la procédure du 16 juillet 2008)* élaborées par le PFPDT dans le cadre de son dispositif d'accompagnement aux organisations (SGPD). Ce « mode d'emploi » se propose de permettre aux personnes appelées à appliquer la LIPAD de mieux saisir l'esprit et les enjeux recouverts par les principes de cette loi, ainsi que les réflexes à acquérir pour s'assurer de leur respect. Il est subdivisé selon les neuf principes généraux en matière de protection des données déductibles de la LIPAD, à savoir:

– légalité;
– transparence de la collecte;
– proportionnalité;
– finalité (principe implicite);
– exactitude;
– communication (transfrontière) des données;
– sécurité des données;
– déclaration des fichiers;
– droits d'accès.

Le *code de bonne pratique* est destiné à être présenté à l'ensemble des services administratifs, puis à les accompagner dans leur pratique.

Nécessité d'une gouvernance

Le développement et l'évolution des prestations en ligne s'assimilant à un projet[25], les e-démarches pourraient *a priori* être gérées par la CGSIC comme le ROGSIC le préconise pour les autres projets informatiques, et, pour les questions plus générales, par la délégation du Conseil d'Etat à l'Internet. Il ne s'agit donc pas de créer de nouvelles structures administratives, mais d'utiliser celles qui existent déjà et de préciser leurs rôles respectifs.

Une gouvernance spécifique, telle que la délégation du Conseil d'Etat peut l'assurer, est nécessaire pour adopter une vision globale et assurer la

[25] *Voir ci-dessus, « Problématiques d'encadrement des projets », pp. 13 s.*

cohérence du financement et de la priorisation des développements en cours de réalisation sur un socle commun. Avant l'AeL, les expérimentations des prestations en ligne se faisaient sans réelle concertation entre les offices, avec le côté disparate propre à tout projet conduit sans lien avec les projets similaires.

Cet encadrement transverse ne justifie pas de modification de la LIPAD.

Information de l'utilisateur, adoption des CGU AeL

La LIPAD fait à plusieurs reprises l'obligation aux responsables des données personnelles d'informer l'utilisateur, que ce soit sur la collecte même de données personnelles le concernant (art. 38, al. 1 LIPAD) que sur l'usage qui en sera fait. Le titulaire des données personnelles doit aussi être orienté sur la personne auprès de laquelle il pourra exercer ses droits d'accès (art. 44 à 46 LIPAD), de correction (art. 47, al. 2, lettre b LIPAD), de suppression (art. 47, al. 2, lettre a LIPAD), de mention (art. 47, al. 2, lettre c LIPAD) des données qui le concernent, ou encore de constatation, d'abstention, respectivement de suppression de tout acte illicite (art. 47, al. 1 LIPAD).

La nécessité d'informer directement l'utilisateur s'est traduite à ce jour par l'adoption de conditions générales d'utilisation (CGU AeL) établies dans un esprit didactique et d'engagement sur les prestations. Mais cela ne suffit pas. Afin de rendre l'administré attentif aux communications de données que sa demande générera d'un service à l'autre au sein de l'administration (« consentement éclairé » de l'art. 35, al. 2 *in fine* LIPAD), l'inscription à un service donné donne lieu à une information sur les flux engendrés et permet de prendre connaissance des services qui seront appelés à collaborer pour que la décision demandée puisse être rendue.

En outre, l'administration doit pouvoir rendre compte de son activité en ligne tant envers sa hiérarchie et ses auditeurs qu'envers l'administré – dont elle gère notamment certaines de ses données personnelles. Il s'agit de renforcer le degré de transparence des dispositifs techniques, ce qui crée une obligation de la DGSI de prendre au côté des métiers la responsabilité de la garantie de la conformité (par rapport aux CGU AeL, à la loi et aux normes de sécurité en vigueur). En outre, pour donner une image cohérente à l'utilisateur / administré et lui faciliter l'apprentissage de ces outils, les départements doivent mettre en œuvre des processus de gestion en ligne similaires les uns aux autres. On rejoint ainsi la préoccupation d'une gestion transversale des prestations en ligne.

Continuité et évolutions

Introduction

Diverses préoccupations liées au changement de paradigme induit par les e-démarches ont été évoquées tout au long du présent rapport : nécessité de maintenir une cohérence technique, logique et visuelle des e-démarches, ainsi que d'assurer le contrôle de leur conformité à la loi (LIPAD, LPFisc, CP), auxquelles s'ajoute le souci d'informer l'administré de ses droits et responsabilités dans ce nouveau cadre. Tout ceci semble plaider en faveur de l'adoption d'une nouvelle loi, propre aux e-démarches et, de manière plus générale, à la communication en ligne entre l'Etat et les administrés. Cette loi ferait office de fédérateur comme l'a fait jusqu'à présent le programme d'impulsion qu'est l'AeL.

Ceci ne veut pas dire qu'il faille renoncer à toute modification de la LIPAD, mais les changements proposés visent plutôt à renforcer l'efficacité de son application qu'à amoindrir à long terme par des dérogations la portée de ses principes.

Modifications à apporter à la LIPAD

Bien que l'expérience accumulée au cours du programme AeL conduise à la conclusion qu'il est possible de respecter les principes de la LIPAD, la mise en œuvre des dix prestations d'impulsion a souligné certaines lacunes concrètes du texte, qu'il pourrait être profitable de corriger.

Conflits entre la LIPAD et la LPD

La LIPAD s'applique à l'administration cantonale genevoise dans le cadre de la politique de transparence et de protection des données personnelles.

Son champ d'application entre en concurrence avec la LPD dans la plupart des échanges entre l'Etat et les tiers (personnes physiques et morales), puisque la LIPAD s'applique à la communication de données par l'administration cantonale aux tiers, alors que la LPD s'applique aux tiers, notamment en matière de communication de données d'un administré à l'administration cantonale. Cela rend difficile dans certains cas la détermination de la loi applicable, et entraîne donc un risque accru en matière de sécurité dans le traitement des données.

C'est pour cela que le Conseil d'Etat s'est déterminé fin 2013 en faveur d'une application de la LPD aux administrations cantonales à l'occasion d'une consultation de la Confédération. Mais une telle mesure n'est plus d'actualité, vu le rejet de ce projet par la plupart des autres cantons; il convient donc d'examiner les aménagements à apporter à la LIPAD pour l'adapter aux enjeux posés par les e-démarches.

Principe de finalité

Il conviendrait en premier lieu de spécifier expressément l'existence du principe de finalité. Celui-ci se trouve par exemple expressément mentionné à l'article 4, alinéa 3 LPD, mais non dans la LIPAD, si ce n'est à travers le principe de licéité, ce qui ouvre la voie à des interprétations réductrices et complique inutilement le débat.

Ce principe de finalité vise à assurer que les données personnelles ne sont traitées que dans le but qui est indiqué lors de leur collecte, but qui est prévu par une loi ou qui ressort des circonstances. Cela suppose, pour chaque flux de données personnelles au sein de l'Etat, que la disposition légale justifiant le transfert (la « tâche légale » de l'art. 35, al. 1 *in fine* LIPAD) existe bien et rende nécessaire une telle transmission de données.

Le contrôle de l'existence d'une tâche légale constitue l'essentiel de l'effort d'organisation au sein de l'administration exigé par le contrôle de la conformité[26]. Or, si le principe de finalité se trouve clairement exprimé dans l'article 4, alinéa 3 LPD et dans la plupart des lois relatives à la protection des données personnelles, il n'est transposé dans la LIPAD que de manière implicite, la finalité d'un traitement se confondant pour le législateur genevois avec les dispositions légales ou règlementaires qui en dictent la nécessité. Cette approche, sans doute juridiquement défendable, a pourtant nuit au respect effectif du principe de finalité, dans un domaine où la pédagogie a toute son importance. Il s'avère donc important de l'inscrire en toutes lettres dans la loi, afin de faciliter son application effective, qui nécessite la collaboration du responsable des données (le « maître des fichiers ») et des acteurs informatiques, qui ne sont pas juristes.

L'article 39 LIPAD, qui explicite un aspect du principe de finalité (pas de transfert de données personnelles d'un office à l'autre au sein de l'Etat ou, *a fortiori*, de l'administration à un tiers qui ne soit justifié par une loi ou un règlement), est à l'heure actuelle difficilement applicable et donne lieu à des querelles d'interprétation. Il devrait être notablement simplifié, en s'inspirant de l'approche adoptée par la LPD.

L'inscription expresse et de manière simplifiée du principe de finalité dans la LIPAD est d'autant plus justifiée si l'on considère l'exigence du caractère *nécessaire* (art. 35, al. 1 et 2, art 36, al. 1, lettre a, et 41, al. 1, lettre a LIPAD) ou *absolument indispensable* du traitement à l'accomplissement d'une tâche légale (art. 35, al. 2 LIPAD) pour pouvoir communiquer des données personnelles d'un service à l'autre. Cette exigence peut sembler

[26] *Voir ci-dessus, « Mise en œuvre d'un SGPD », pp. 7 s.*

disproportionnée si le principe de finalité ne représente qu'un aspect implicite du principe de légalité, dès lors que nous vivons à une époque où la gestion de toutes les tâches légales de l'administration se fait nécessairement par le biais de l'informatique. Pour éviter de renoncer à cette exigence, il convient là encore d'inscrire expressément le principe de légalité dans la loi.

Par ailleurs, on sait que la mise en œuvre de e-démarches implique un décloisonnement apparent de la structure des différents départements et services de l'administration au profit d'une logique de prestation, ce qui nécessite une plus grande collaboration au sein de l'administration. Se pose donc la question de l'obtention de l'accord du bénéficiaire de la prestation quant à la transmission de son dossier à plusieurs services. Lorsque le titulaire des données personnelles transmises pour rendre la prestation n'est autre que le demandeur de la prestation, l'accord éclairé est donné par l'intéressé lors de son inscription à l'e-démarche correspondante. En effet, l'utilisateur est rendu attentif à cette occasion à l'ensemble des services appelés à collaborer dans le cadre de cette e-démarche. Il lui est alors demandé de donner son accord à la transmission des données nécessaires, accord donné pour toutes les demandes à venir de ce type. Faute d'une telle autorisation expresse et éclairée, le processus d'inscription à l'e-démarche est interrompu.

La question est plus délicate s'il est nécessaire de transmettre des données de tiers pour délivrer la prestation requise. Dans ce cas, c'est à la loi de fond justifiant le transfert d'informations d'un office à l'autre de prévoir le transfert nonobstant l'accord exprès du tiers concerné, comme le fait par exemple l'article 6 de la loi sur les bourses et prêts d'études (C 1 20). Là encore, une modification de la LIPAD ne semble pas nécessaire pour résoudre cette problématique.

Partage des responsabilités

Les événements relatifs à la protection des données qui ont paru le 26 janvier 2013 dans la presse (prétendus accès aux données des contribuables genevois par une société française, ce que le Conseil d'Etat avait démenti) ne font que confirmer l'absence de partage clair des responsabilités entre DGSI, offices départementaux responsables de l'organisation de l'information (OROI), PPDT et responsables LIPAD. De manière générale, cette problématique est renvoyée à une résolution purement technique par les métiers, et, réciproquement, à une résolution purement métier par les techniciens, ce qui contribue à une dilution des responsabilités et à un attentisme dangereux. Cette situation menace à terme la confiance que le public met dans l'administration genevoise, considérée à juste titre comme maître des fichiers qui le concernent. Ce défaut a un impact

important sur l'image de l'Etat en général, ce que montrent bien les attaques désordonnées de la presse, atteignant à l'époque indistinctement la DGSI, le DSE et l'AFC.

Or, contrairement à la LPD, la LIPAD ne gère pas le partage des responsabilités entre le métier (responsable des données, ou « maître des fichiers » au sens du ROGSIC) et leur gestionnaire opérationnel (en l'occurrence, la DGSI). Cette lacune – sans doute la principale de la LIPAD – a pesé sur la mise en conformité à la loi, chacun des acteurs étant tenté d'attribuer aux autres la responsabilité de l'ensemble des aspects liés à la protection de données.

C'est l'adoption du ROGSIC qui a indirectement comblé cette lacune; la responsabilité du maître des fichiers (art. 10, al. 1, lettre c, et 10, al. 2 ROGSIG), celle de la DGSI (art. 8 ROGSIC) et les tâches à mener de concert entre les deux entités (art. 6, al. 1, lettre a, ch. 2 ROGSIC) y sont en effet clairement distinguées. Le ROGSIC et le RIPAD ayant un champ d'application plus restreint que la LIPAD, il serait fort souhaitable d'intégrer ces dispositions ou leur équivalent dans la loi.

En matière de partage des responsabilités à l'interne de l'Etat, il est rappelé à titre liminaire que les parties prenantes sont les suivantes : la DGSI (en particulier la direction sécurité de l'information et événements spéciaux, le service réseaux-télécommunication, le service architecture, le service juridique et le service sécurité opérationnelle), le PPDT, les OROI départementaux, les responsables sécurité des systèmes d'information, le comité de sécurité des systèmes d'information (ComSec-SI), ainsi que les responsables LIPAD.

Il est proposé un partage de responsabilité selon quatre axes :

1. La conception du système de gestion de la sécurité des données et l'élaboration du SGPD (modèle de conformité aux principes et dispositions opérationnelles de la LIPAD) : ils relèvent de la responsabilité de la DGSI, en collaboration avec les départements.
2. Le traitement des données métiers (soit la mise en œuvre de règles de traitement conformes au SGPD) : elle doit revenir à l'entité endossant le rôle de maître de fichiers, soit l'office métier responsable des données, aidé des OROI et RSI départementaux, ainsi que des responsables LIPAD. Cette gestion emporte une responsabilité tant envers leur hiérarchie qu'envers les administrés quant au respect de la LIPAD.
3. La gestion technique de l'information et du support, soit la gestion des données permanentes sur l'infrastructure (comprenant notamment les serveurs, bases de données, les journaux, les supports de sauvegarde et

d'archivage de données), laquelle porte sur la sécurité des accès physiques et logiques (connexion directe aux machines et accès à distance ou externe), à travers le système de management de la sécurité de l'information (SMSI), doit revenir à la DGSI, en collaboration avec les responsables départementaux de la sécurité de l'information (RSI). Cette gestion emporte une responsabilité tant envers les départements qu'envers les administrés; le contrôle par la DGSI de son activité portera aussi sur les prestations de service telle que l'assistance (support) et la maintenance.

4. La vérification de la conformité au SGPD et la tenue de rapports de contrôle en matière de protection des données à l'attention des offices métiers responsables des données, aidés des OROI départementaux revient au gestionnaire du socle, soit, là encore à la DGSI, charge aux offices métiers responsables des données de tirer les conséquences de ces rapports et de mettre en œuvre les politiques correctives qu'ils suggéreront peut-être, ainsi que d'en informer le citoyen.

Le partage clair et adéquat des responsabilités de chacun doit s'accompagner d'une organisation adéquate, à même de garantir son application.

La question du transfert des responsabilités s'avère particulièrement épineuse s'agissant des transferts en chaîne de données personnelles et justifie d'autant plus que la loi clarifie la situation. Prenons un exemple théorique. Si l'AFC transmet au registre foncier (RF) les adresses à jour des propriétaires d'immeuble et que l'office cantonal de l'énergie (OCEN) récupère auprès du RF l'identité des propriétaires d'immeuble, ainsi que leurs adresses, la question de la responsabilité se pose. Est-ce que l'OCEN peut requérir les adresses des propriétaires d'immeubles directement auprès de l'AFC, ou est-il est en droit d'exiger du RF la garantie que les adresses transmises sont bien les dernières qui lui ont été communiquées par l'AFC ? Ces transferts en chaîne sont en outre liés à la gestion des systèmes d'information, et posent la question des référentiels de données : quel office est-il garant pour les autres de tel type de données ?

Cette problématique pourrait être résolue par l'ajout dans la LIPAD d'une disposition exposant les principes applicables en matière de responsabilité entre l'office émetteur, l'office destinataire, l'office destinataire en seconde ligne et la DGSI, disposition qui traiterait également des garanties de qualité des données transmises qui y seraient assorties. S'y ajouterait, dans un texte

législatif propre à la communication en ligne[27], une autre disposition indiquant les circonstances dans lesquelles une convention de transfert de données personnelles ou confidentielles *doit* être passée entre offices. Le contenu des conventions spécifiques passées entre offices pourrait alors se limiter à rappeler la base légale justifiant le transfert de données, le genre (personnelles / confidentielles) et la qualification juridique (données personnelles, données personnelles sensibles, autres données confidentielles) des données transmises, le mode technique de transmission convenu, la périodicité des mises à jour, ainsi que le rappel du régime de responsabilité prévu par la LIPAD applicable au cas concret, permettant ainsi de s'assurer que les offices concernés ont la même lecture du transfert de données auquel ils sont partie.

Nécessité d'une régulation législative propre à la communication en ligne

En 2006 déjà, il était relevé que les deux principaux obstacles à l'administration en ligne en Suisse étaient autant l'absence d'un cadre juridique approprié relatif à « l'administration électronique » que l'existence de dispositions légales incompatibles avec elle[28]. Par ailleurs, le comité de pilotage de la cyberadministration suisse a souligné lors de sa séance du 4 décembre 2014 l'importance qu'il accorde aux bases légales dans le cadre de la cyberadministration. Il indique que pour permettre l'atteinte des objectifs fixés dans le domaine de la cyberadministration, l'existence de bases légales appropriées et à jour, garante de la nécessaire légitimité démocratique, est essentielle[29].

A Genève, l'ancrage juridique des prestations en ligne de l'AeL a été effectué de manière volontairement temporaire, ou sous forme d'exception. En l'état, il se révèle inadapté pour la suite, puisqu'il s'agit de régler de façon générale et transverse non seulement la communication en ligne entre les différents services de l'Etat, ainsi qu'entre l'Etat et les tiers, mais aussi la gestion des données permanentes impliquées par les prestations rendues en ligne. De plus, des règlements disparates traitent séparément de sujets similaires: ainsi, le règlement relatif aux déclarations d'impôt établies à l'aide d'outils informatiques (rs/GE D 3 17.03 – RDIOI) traite du cas spécifique des

---

[27] *Voir ci-dessous, « Nécessité d'une régulation législative propre à la communication en ligne », p. 36 ss*

[28] *VERNIORY Jean-Marc, « L'Administration électronique en Suisse », Collection spéciale de l'Institut Suisse de Droit Comparé (ISDC), vol. 54 (2006), Rapports suisses présentés au XVII^e Congrès international de droit comparé (Utrecht, 16 au 22 juillet 2006), Shulthess, Bâle 2006, pp. 271-292.*

[29] *https://www.news.admin.ch/message/index.html?lang=fr&msg-id=55576*

déclarations fiscales, tout en reprenant les mêmes principes que ceux exposés par le règlement sur la communication électronique (rs/GE E 5 10.05 – RCEL).

Comment répondre à ce défi de manière à la fois globale, cohérente et pérenne ? Diverses solutions ont déjà été adoptées par des Etats ou des cantons voisins. L'étude comparative des solutions mises en œuvre par les cantons de Neuchâtel, du Jura et de Zurich, ainsi que par la France, l'Autriche et la Finlande, a permis de dégager la solution qui semble la meilleure pour Genève[30].

L'option préconisée

Il est possible d'encadrer les e-démarches de plusieurs manières : par une loi topique, de manière disparate, par l'insertion, dans chacune des lois de fond concernées, d'une disposition permettant de rendre les prestations qu'elles décrivent par la voie numérique, ou encore par une approche contractuelle, sous forme de CGU.

Il apparaît d'emblée que la gestion des prestations en ligne par des dispositions disparates n'est guère satisfaisant et entraîne un manque de visibilité et de transparence pour l'administré, sans parler de la difficulté pour le législateur à mettre à jour le *corpus* législatif en fonction des avancées des e-démarches. C'est pourtant ce qui correspond à l'état actuel de la législation genevoise en la matière.

La législation genevoise traite en effet des prestations en ligne par un ensemble de dispositions disparates (art. 18A LPA, RCEL, RDIOI, art. 69 LIPAD), ce qui pose la question de leur cohérence. La coordination et l'articulation entre les instruments de divers niveaux (loi, règlement, conditions générales d'utilisation) n'est actuellement pas assurée et de nombreux doublons existent. La question de l'identification est ainsi traitée à la fois par le RCEL, par le RDIOI et par les CGU.

Une telle situation ne saurait perdurer trop longtemps au risque de compromettre la dynamique instaurée par l'AeL; d'une dynamique d'exception et d'expérimentation, il s'agit de passer résolument à une dynamique opérationnelle et transverse grâce à l'expérience acquise.

Les textes actuellement en vigueur ne suffisent pas à doter la communication électronique d'une base formelle réglant avec clarté son fonctionnement et confirmant les garanties que le Conseil d'Etat entend

30 *La description détaillée des solutions adoptées figurera dans la partie générale de l'exposé des motifs du projet de loi sur l'Administration en ligne dont il est question ci-dessous.*

donner aux utilisateurs des futures e-démarches. Traiter de manière durable et cohérente ces questions essentielles à travers les seules CGU AeL ne semble guère plus indiqué. Du reste, dans leur propre rapport, le PPDT et la Commission consultative en matière de protection des données, de transparence et d'archives publiques appellent chacun de leur côté une telle loi de leurs vœux.

La première nécessité consiste à donner une base juridique en matière de gouvernance et de qualité des prestations en ligne, de manière notamment à assurer une véritable gestion de la conformité des e-démarches, ainsi qu'une prise en compte dès leur conception des exigences légales. *Cela peut se faire sans nécessiter la création de nouvelles instances de gouvernance, mais en désignant celles qui existent déjà*. Il s'agit également d'accorder une visibilité suffisante aux garanties que le Conseil d'Etat avait données aux citoyens en matière de e-démarches dans son discours de Saint-Pierre. Le principal but poursuivi est d'instaurer la confiance nécessaire au déploiement des e-démarches. Vu l'importance qu'ils recouvrent, les grands principes de l'AeL, dont on a vu qu'ils dépassent le cadre de l'organisation de l'administration et concernent également les relations directes de l'administration aux administrés, doivent trouver ancrage dans une loi au sens formel.

Le Conseil d'Etat a le souci, en fin de programme AeL, d'inscrire de manière pérenne la possibilité pour l'administration genevoise d'effectuer des prestations en ligne et d'admettre ouvertement le principe général d'une gestion des prestations sous forme de e-démarches. A cette fin, le Conseil d'Etat entend déposer un projet de loi formelle qui règlera pour l'ensemble de l'Etat la question des prestations en ligne entre services et entre l'Etat et les tiers.

Un tel système sera à même de nourrir la confiance des citoyens, en profitant du meilleur des deux systèmes : la loi pour garantir les principes, tant envers l'administré qu'au sein de l'administration, les CGU pour régler les questions plus concrètes et engager l'utilisateur des e-démarches dans un rapport plus individuel.

Les changements de loi à prévoir

La loi préconisée envisageant les e-démarches dans une perspective transversale et non sous forme d'exception, les alinéas 4 et 5 de l'article 18A LPA (rs/GE E 5 10) devraient être modifiés de façon à renvoyer à cette nouvelle loi; de même, le RCEL (rs/GE E 5 10.05), adopté le 3 février 2010 pour concrétiser l'article 18A LPA, devra être abrogé. Ces dispositions abordent les prestations en ligne comme des exceptions, et non en tant que principe général de communication, ce qui s'oppose de manière frontale au

développement des prestations en ligne en tant que politique publique. L'établissement d'une liste des « domaines dans lesquels la communication électronique est admise » est de plus voué à l'échec – du moins à l'obsolescence constante[31], ce qui n'est guère souhaitable. Il ne tient surtout pas compte du changement de paradigme opéré par les e-démarches ni, de manière plus générale, des changements techniques opérés ces quinze dernières années à travers l'Internet.

Conclusion

Le programme d'impulsion qu'est l'AeL a permis de démontrer qu'il est possible de proposer des prestations en ligne sans déroger aux principes de la LIPAD. Une telle démarche nécessite toutefois la mise en place d'une organisation et d'outils permettant de contrôler et de garantir la conformité des e-démarches à la loi.

Le Conseil d'Etat proposera, dans un souci de cohérence, d'adopter une loi sur l'Administration en ligne tenant compte de l'expérience acquise au cours du programme d'impulsion qu'est l'AeL et d'inscrire l'évolution des e-démarches dans un cadre plus pérenne, tirant parti de l'organisation mise en place par le ROGSIC. La LIPAD serait de son côté complétée par l'expression du principe de finalité et par une disposition réglant la question de la responsabilité des acteurs. L'adoption de la loi topique serait accompagnée de l'allègement des CGU AeL actuelles et de l'abrogation du RCEL.

Au bénéfice de ces explications, le Conseil d'Etat vous invite, Mesdames et Messieurs les Députés, à prendre acte du présent rapport.

AU NOM DU CONSEIL D'ÉTAT

La chancelière :	Le président :
Anja WYDEN GUELPA	François LONGCHAMP

[31] *C'est un fait que la liste de prestations mentionnées actuellement dans le RCEL n'est pas à jour depuis longtemps et n'a pas tenu compte des e-démarches.*