Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

KONFERENZ DER KANTONSREGIERUNGEN
CONFERENCE DES GOUVERNEMENTS CANTONAUX
CONFERENZA DEI GOVERNI CANTONALI
CONFERENZA DA LAS REGENZAS CHANTUNALAS

Rapport final
Solutions et mesures

Projet prioritaire :	B1.02 Bases légales
Nom du projet :	Bases légales de la cyberadministration en Suisse : conception
Organisation chef de file :	Office fédéral de la justice
Date :	Mai 2012

Abréviation du nom du rapport final	**BLA**
Classification *	nicht klassifiziert
Statut **	en traitement
Nom du projet	**Konzept Rechtsgrundlagen für E-Government in der Schweiz**
Abréviation du nom du projet	RGeGov (B1.02)
Chef de projet	Urs Paul Holenstein
Mandant	E-Government Suisse
Auteur	U. Bürge (BUE)
Vérification	L. Fässler, H. Münst, D. Stettler, ffOs (OCF)

* non classifié, interne, confidentiel
** en traitement, en vérification, terminé

Contrôle des modifications, vérification, approbation

Version	Date	Description, remarques	Nom ou rôle
0.1	18.7.2011	Projet établi sur la base de la séance du 6.6.2011	U. Bürge
0.3	5.9.2011	Remaniement selon l'entretien du 16.8.2011	Contribution HUP, MUE, FAE ; U. Bürge
0.4	19.9.2011	Remaniement selon l'entretien du 5.9.2011	Contribution HUP, MUE, FAE, STD ; BUE
0.5a	6.10.10.2011	Refonte, version pour envoi aux OCF	Contribution HUP, MUE, FAE ; U. Bürge
0.8	30.3.2012	Rapport remanié selon la contribution du groupe de travail	Contribution du groupe de travail OCF ; U. Bürge
1.0	7.5.2012	Version pour livraison au mandant	U.P. Holenstein

Objectif du présent document

Le présent rapport fait la synthèse des résultats de la dernière phase des travaux portant sur le projet prioritaire « B1.02 Bases légales ». Depuis la fin de l'automne 2010, les résultats obtenus jusqu'ici ont été classés selon leur ordre de priorité, évalués et, si possible, transformés en mesures prioritaires. Celles-ci sont présentées au mandant sous la forme de solutions.

En se fondant sur le présent document, le mandant – E-Government Suisse – décidera des prochaines étapes et, le cas échéant, pourra confier les mesures de mise en œuvre aux OCF.

Définitions, acronymes et abréviations

Terme	Définition
DFJP	Département fédéral de justice et police
eCH	Association développant et adoptant des normes en matière de cyberadministration et de cybersanté en Suisse (www.ech.ch)
E-Government Suisse	Organisation chargée de la mise en œuvre de la stratégie suisse de cyberadministration, conformément à la convention-cadre conclue entre la Confédération et les cantons. Elle se compose d'un comité de pilotage, d'un conseil des experts et d'une direction opérationnelle. (www.egovernment.ch/)
eJustice.CH	Association eJustice.CH (anciennement Association suisse pour le développement de l'informatique juridique, ASDIJ, www.eJustice.CH)
IAM	*Identity and Access Management* (gestion des identités et des accès) ; gestion des identités ; système permettant de gérer les identités et l'accès aux services.
LAN	*Local Area Network* ; réseau local reliant chaque place de travail
LPD	Loi sur la protection des données, RS 235.1
NAVS13	Nouveau numéro AVS à 13 chiffres, introduit en 2007
OCE-PA	Ordonnance du 18 juin 2010 sur la communication électronique dans le cadre de procédures administratives, RS 172.021.2
OCE-PCPP	Ordonnance du 18 juin 2010 sur la communication électronique dans le cadre de procédures civiles et pénales et de procédures en matière de poursuite pour dettes et de faillite, RS 272.1
OFCOM	Office fédéral de la communication
OFIT	Office fédéral de l'informatique et de la télécommunication ; fournisseur de prestations informatiques à l'échelon de la Confédération
OFJ	Office fédéral de la justice
PFPDT	Préposé fédéral à la protection des données et à la transparence
RS	Recueil systématique du droit fédéral (www.admin.ch/ch/f/rs/rs.html)
SCSE	Loi fédérale du 19 décembre 2003 sur les services de certification dans le domaine de la signature électronique, RS 943.03
SuisseID	Norme suisse pour l'identité électronique, comprenant l'authentification, la signature qualifiée et la preuve d'identité (www.SuisseID.ch)
USIC	Unité de stratégie informatique de la Confédération

Table des matières

1 Mandat, problématique

Quiconque se penche sur la concrétisation d'un projet de cyberadministration, constate souvent que les problèmes juridiques gênent les travaux et que l'absence de bases légales retarde voire empêche leur réalisation.

Eu égard à ce constat, le projet « B1.02 Bases légales » a été intégré, dans le cadre de la stratégie suisse de cyberadministration, à la liste des projets prioritaires. Il a d'abord été traité par la direction opérationnelle d'E-Government Suisse, puis placé sous la responsabilité de l'Office fédéral de la justice (OFJ).

Il s'agit, dans les grandes lignes, de savoir comment apaiser le malaise ressenti par les acteurs de l'environnement cyberadministratif vis-à-vis des bases légales et d'autres problématiques juridiques. Il s'agit aussi de vérifier s'il est nécessaire d'adapter les bases légales ou d'en adopter de nouvelles pour mettre en œuvre les projets de cyberadministration et, si tel est le cas, dans quels domaines et à quel niveau (fédéral ou cantonal).

Une problématique similaire est apparue lors de la mise en application de la Stratégie pour une société de l'information en Suisse. Le Conseil fédéral a donc chargé le Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC), puis le Département fédéral de justice et police (DFJP) de préparer les bases légales nécessaires à la mise en œuvre de la stratégie. Ces deux mandats donnent lieu à des activités dont les problématiques se recoupent partiellement. La « société de l'information » englobe davantage de domaines. Outre la cyberadministration, elle aborde des sujets comme la cybersanté, le commerce électronique (e-commerce) ou l'intégration numérique. La manière dont les travaux s'harmonisent entre eux et se complètent est décrite ci-dessous.

2 Méthode, étapes réalisées jusqu'ici

La problématique des bases légales se décline en deux volets. Le tableau synoptique suivant met en lumière les activités et les jalons principaux de chacun d'entre eux.

	Cyberadministration : B1.02 Bases légales	**Société de l'information : Consolidation des bases légales**
2008		5.12. : décision du CF : mandat confié au DETEC
2009	18.6. : atelier « C » avec les OCF, bases légales -> Procès-verbal (Eicher) ; -> Résultats (Fässler), avec synopsis	Groupe de travail interdépartemental -> déc. 2009 : rapport «Consolidation des bases légales »
2010	4.11. Comité de pilotage : attribution de la direction du projet à l'OFJ	16.3. : OFJ : Guide pour l'élaboration des bases légales 11.6. : décision du CF : attribution de la direction du projet au DFJP
2011	11.3. : lettre d'information aux OCF, cantons + enquête sur la nécessité de légiférer 6.6. : atelier d'analyse interne ; -> projet, rapport Solutions et mesures oct./nov. : ateliers avec les OCF et les préposés cantonaux à la protection des données	6.7. : décision du CF : mandats confiés au DFJP : - avant-projet sur la signature électronique - rapport sur la collaboration informatique entre la Confédération et les cantons - conception organisationnelle et financière des infrastructures de base de la cyberadministration - rapport sur l'identificateur de personnes dans le domaine de la justice

3 Problèmes, attentes, objectifs

Un projet de cyberadministration peut, en fonction de l'objectif concret et de l'organisation, comporter de nombreux problèmes ou activités d'ordre juridique.

Les situations peuvent différer selon la nature de la mission :

- élaboration d'une base légale ;
- abrogation d'une disposition existante qui rendrait impossible le processus électronique (par ex. prescriptions sur la forme) ;
- rédaction de règlements juridiques pour la mise en œuvre et l'exploitation d'une nouvelle application (par ex. pour que la protection des données et le principe de la transparence soient respectés) ;
- réalisation d'une procédure d'autorisation ou de déclaration (par ex. pour l'utilisation du NAVS13).

Citons quelques exemples concrets d'activités dans le domaine juridique :

- création de bases légales en vue de permettre une procédure électronique voire de contraindre les participants à l'appliquer ;
- adaptation des prescriptions de forme pour le passage à la procédure électronique ;
- établissement de bases légales pour le financement d'un système ;
- élaboration de la base légale pour une nouvelle banque de données, y compris les règlements relatifs au traitement des données, à la maîtrise des données, aux droits d'accès et à la protection des données ;
- création de la base légale pour l'accès à une banque de données existante, contenant des données personnelles (particulièrement sensibles) ;
- règlementation relative aux publications en ligne et à leur suppression (« droit à l'oubli numérique ») ;
- règlementation du classement des documents et mise en œuvre du principe de la transparence ;
- règlementation de la gestion des dossiers et de l'archivage des dossiers électroniques.

3.1 Description des problèmes, attentes

Les problèmes décrits dans les différentes phases du projet B1.02 – et de celui sur la société de l'information - reflètent toutes les questions juridiques exposées ci-dessus, susceptibles de se poser dans le contexte de projets de cyberadministration.

Par exemple :

- les bases légales régissant le passage à la procédure électronique, et en particulier les prescriptions détaillées sur la forme, doivent figurer dans une norme de rang supérieur ;
- la création d'un recueil de données ou l'accès à un recueil en exploitation doivent se fonder sur des bases légales fédérales ou cantonales existantes ;
- le financement de projets de cyberadministration communs à la Confédération et aux cantons et la répartition des coûts doivent faire l'objet d'une réglementation uniforme ;
- l'usage du NAVS13 en tant qu'identificateur de personnes dans toutes les applications de cyberadministration doit se fonder sur des bases légales fédérales.

Les problèmes et les attentes identifiés dans le cadre des deux projets en cours sur les bases légales ont été résumés dans [1] pour la société de l'information et dans [2] pour la cyberadministration (B1.02).

3.2 Enquête et prise de position sur la nécessité de légiférer

La deuxième enquête, menée en mars 2011 auprès des OCF, mettait l'accent sur la nécessité de légiférer et sur l'évaluation des différentes mesures proposées en vue de supprimer les lacunes et les problèmes identifiés jusqu'ici. Les OCF, les centres de compétences cantonaux en matière de cyberadministration et les préposés cantonaux à la protection des données ont été invités à prendre position sur une liste complète de champs d'action et de mesures de mise en œuvre prioritaires.

L'enquête [3] et une synthèse de l'évaluation [4] figurent en annexe.

La plupart des participants ont admis qu'il était nécessaire de légiférer. Ils ont salué les mesures mais exclu tout soutien financier de la part de leurs services.

Cependant, leur évaluation diverge en de nombreux points. Le service de cyberadministration et le service informatique d'un même canton ont, par exemple, une opinion contraire sur plusieurs questions.

Il ressort dans l'ensemble que les « techniciens » attendent énormément des mesures proposées alors qu'en revanche, les « spécialistes du droit » (par ex. les préposés à la protection des données) estiment que les bases et les instruments nécessaires sont déjà disponibles, mais que le bât blesse au niveau de leur application et de leur concrétisation.

3.3 Thèses sur la situation et sur la nécessité de légiférer

Tous s'accordent sur le fait qu'il existe un malaise en ce qui concerne les bases légales. Toutefois, il est difficile de faire une synthèse des prises de position et d'en tirer des mesures prometteuses et praticables pour améliorer la situation. D'une part, les participants décrivent, de manière plausible et claire, les obstacles et les blocages inutiles. D'autre part, ils se contredisent et ne disposent pas de connaissances suffisantes des concepts politiques et juridiques fondamentaux ni des méthodes à employer ou espèrent des solutions miracles et des modifications en profondeur.

Etant donné que, pour les raisons évoquées, les conclusions ne sont pas solides, elles sont formulées, ci-dessous, sous la forme de thèses. Celles-ci ne valent souvent que partiellement et peuvent, dans certaines circonstances, être en contradiction avec d'autres thèses.

> **Thèse 1** : la collaboration entre les « techniciens » et les « spécialistes du droit » fonctionne mal. Ces derniers parviennent uniquement à évoquer les difficultés ou les lacunes au niveau juridique. Toutefois, ils ne proposent aucun soutien adéquat ni n'indiquent comment surmonter les obstacles juridiques.
>
> La plupart du temps, aucune personne ayant une formation juridique n'est affectée à l'équipe de projet. De plus, il n'y a pas de collaboration effective avec le service juridique.

Selon de nombreux chefs de projet, les spécialistes du droit se limitent à énumérer les problèmes et les obstacles d'ordre juridique. Ils ajoutent que les juristes ne sont plus disponibles lorsqu'il s'agit de chercher et de développer une solution ou qu'ils ne connaissent pas suffisamment les questions techniques et organisationnelles. Il n'existe aucune antenne de soutien en cas de questions juridiques, formée spécifiquement et capable de trouver des solutions dans les limites légales. Si soutien juridique il y a, il est souvent tardif et ne dure pas jusqu'à la phase de mise en exploitation.

Thèse 2 : il est fréquent que les responsables de la technique et de l'organisation n'aient pas les connaissances minimales requises des principes ou des concepts politiques ou juridiques fondamentaux, tels que le principe de la légalité[1], de la proportionnalité[2] ou de l'affectation obligatoire[3].

Il en résulte que, dans le cas concret, ils ne sont pas en mesure d'évaluer correctement les problèmes juridiques. Ils ne font pas la différence entre une lacune facilement supprimable et une barrière politique fondamentale. Les questions juridiques leur paraissent très opaques et génèrent de la frustration.

Tout comme les juristes qui ne peuvent guère évaluer ce qui, d'un point de vue technique, est facilement ou difficilement soluble voire insoluble, les chefs de projet technique ne sont, eux non plus, pas à même d'estimer quelle est la nature des problèmes juridiques dans le cas concret et comment les résoudre. Cette situation peut faire naître un sentiment de détresse et d'impuissance.

Thèse 3 : ce que les participants au projet perçoivent comme une lacune ou un obstacle juridique et déplorent en tant que tel, constitue très souvent une barrière voulue par le législateur. Son but est d'amener l'instance compétente à expliquer dans le détail pourquoi elle a besoin de l'application ou d'un accès aux données.

Dans ce contexte, on peut mentionner l'accès protégé à des données personnelles, parfaitement réglementé. Il est demandé au législateur compétent – cantonal la plupart du temps –d'approuver explicitement tout nouvel accès à des données personnelles. Il s'agit là d'une mesure politiquement voulue. Une base légale qui garantirait un accès aux données personnelles à partir de toutes les applications de cyberadministration n'est guère envisageable puisqu'elle enfreindrait plusieurs principes essentiels.

L'idée fréquemment formulée d'un portail client central s'étendant à toute l'administration se heurterait à une objection similaire. En l'état actuel des discussions politiques, il ne semble pas réellement souhaitable que toutes les données d'une personne, tous domaines administratifs confondus – des impôts à la police en passant par le système de santé – soient regroupées en un seul et même lieu. L'utilité d'un projet de cette nature doit être pesée, au niveau politique, en tenant compte d'autres principes, tels que le principe de la proportionnalité[2] ou de l'affectation obligatoire[3], ainsi que des prescriptions relatives à l'obligation de garder le secret. Le cas échéant, une décision s'impose pour savoir si le projet est vraiment souhaitable ou non.

Thèse 4 : les acteurs préconisant que la Confédération résolve les problèmes juridiques placent la barre trop haut et ne prennent pas en compte le cadre juridique applicable.

Il est en grande partie impossible de répondre à des attentes de solution panacée. Il en résulte un grand potentiel de frustration.

Par exemple, une loi fédérale régissant la cyberadministration de manière exhaustive remettrait en question, dans plusieurs domaines, la répartition des compétences inscrite dans la Constitution et le

[1] Les actions de l'Etat doivent toujours se fonder sur une base légale qui contient des dispositions suffisamment précises et qui a été promulguée par l'organe compétent.

[2] Les actions de l'Etat doivent être appropriées et nécessaires pour atteindre un objectif d'intérêt public. Ce principe s'applique tant à la législation qu'à l'application dans le cas concret.

[3] Dans ce contexte : les données ne doivent être utilisées qu'aux fins pour lesquelles elles ont été acquises.

principe de subsidiarité[4]. Les limites constitutionnelles du droit privé sont plus étendues, puisque la Confédération dispose de compétences législatives exhaustives dans ce domaine. Cela dit, il faut là aussi poser les bases au niveau de la loi avant de pouvoir débuter la mise en œuvre. La réglementation fédérale actuelle de l'acte authentique électronique prouve que les limitations sont souvent strictes. En effet, bien qu'une règlementation à l'échelon fédéral soit réclamée de toutes parts, on peut, selon les prescriptions en vigueur, uniquement régir les exigences techniques à des fins d'interopérabilité. Il incombe pour l'instant aux cantons de réglementer tous les autres aspects.

> **Thèse 5** : bien qu'il existe des bases légales, des informations ou des exemples relatifs au traitement des questions juridiques dans les projets de cyberadministration, ces documents demeurent souvent inconnus.
> Ces informations ne sont pas archivées de manière satisfaisante.

Un exemple illustre ce fait : la majorité des personnes interviewées ont répondu par l'affirmatif à la question de savoir s'il convenait d'élaborer un « guide relatif au traitement de données personnelles et aux bases légales formelles ». Aucun des participants ne semblait savoir qu'un document de ce type existait déjà et avait déjà été publié.[5] (Le titre de ce document, au demeurant très instructif, en est peut-être la cause).

4 Limites des actions possibles

Puisque les discussions sur les bases légales de la cyberadministration ont lieu à l'échelon fédéral, on pourrait penser de prime abord que la solution réside dans une base légale au niveau fédéral. Les enseignements tirés dans le cadre du présent projet mettent cependant en évidence, dans le prolongement des thèses susmentionnées, que seule une infime partie des problèmes peut être réglée au moyen d'une législation fédérale. Aussi la grande partie d'entre eux doit-elle être résolue, bon gré mal gré, à d'autres niveaux. Les autres solutions sont énumérées brièvement ci-dessous, puis expliquées et décrites dans des chapitres séparés.

1. Solution au niveau du projet : que cela plaise ou non aux chefs de projet, une grande partie des questions portant sur les bases légales de la cyberadministration doivent être réglées directement dans le contexte du projet, que ce soit parce que la base légale existe déjà mais qu'elle n'est pas appliquée correctement ou parce que le législateur veut que certaines questions juridiques soient clarifiées pour chaque application et qu'une décision soit prise pour chacune d'entre elles.
2. Solution au niveau cantonal : l'ordre constitutionnel établi (fédéralisme et principe de subsidiarité) attribue la compétence aux cantons dans les situations normales et à la Confédération dans des cas exceptionnels explicitement définis. Des réglementations fédérales ne sont donc admises – pour la cyberadministration également – que dans des domaines très précis. Des modèles de lois ou une coordination peuvent permettre d'utiliser des synergies et constituer un soutien pour chaque canton.

Les limites posées à une solution au niveau fédéral sont réelles, strictes et efficaces. Sous l'angle du présent projet, elles restreignent considérablement les objectifs qui peuvent être atteints et renferment ainsi un grand potentiel de frustration pour les acteurs concernés. Néanmoins, il ne sert à

[4] Dans ce contexte : la responsabilité d'une action doit être allouée à l'entité du niveau le plus bas capable de résoudre le problème d'elle-même (communes, cantons, Confédération).

[5] Guide pour l'élaboration des bases légales nécessaires pour exploiter un système de traitement automatisé de données personnelles [7]
(http://www.ejpd.admin.ch/content/ejpd/fr/home/themen/staat_und_buerger/ref_legistik/ref_andere_hilfsmittel.html)

rien d'entretenir les attentes en laissant penser que la solution aux problèmes juridiques viendra « d'en haut ».

4.1 Mesures à l'échelle cantonale

S'agissant des mesures à l'échelle cantonale, les acteurs mentionnent, de manière récurrente, deux champs d'actions :

Réglementation pour les essais pilote : presque tous les acteurs cantonaux exigent ou recommandent l'inscription, dans les lois cantonales sur la protection des données, d'une réglementation comparable à celle de l'art. 17*a* LPD, qui autoriserait, à certaines conditions et pour une durée limitée, la réalisation d'essais pilotes avec accès à des données personnelles, avant que les bases légales formelles nécessaires soient disponibles. De nombreux responsables cantonaux de la protection des données conseillent également ce type d'adaptations. Les modèles sont connus. Cette mesure doit être concrétisée au niveau légal dans chaque canton séparément.

Loi sur la cyberadministration : certains cantons ont déjà discuté de la question de savoir s'il était indiqué de promulguer une vaste loi sur la cyberadministration en tant que législation-cadre pour plusieurs domaines. D'autres cantons se penchent actuellement sur ce point. Il existe des exemples bien documentés de décisions en faveur d'une loi de cette nature ou contre celle-ci. Elles fournissent des informations et des indications intéressantes pour chaque champ d'action. La teneur de lois sur la cyberadministration peut varier très fortement. Elles contiennent souvent en premier lieu des réglementations organisationnelles et financières ayant trait à la collaboration entre le canton et les communes.

En 2009, le canton de Schwyz a adopté une loi de ce genre (voir la loi et les explications y afférant à l'adresse : http://www.sz.ch/documents/Broschuere_27_09_09_GzD.pdf ; en allemand uniquement). Elle régit en priorité les compétences et le financement de projets de cyberadministration.

Dans le canton d'Appenzell Rhodes-Extérieures, la consultation relative à une loi sur la cyberadministration s'est achevée en août 2011. La fondation d'un centre informatique commun pour le canton et les communes y occupe une place prépondérante (http://www.ar.ch/politische-rechte/vernehmlassungen/abgeschlossene-vernehmlassungen ; en allemand uniquement).

Dans la Principauté de Liechtenstein, une loi de cette nature a été élaborée en 2011 (entrée en vigueur en 2012, cf. http://www.gesetze.li/get_pdf.jsp?PDF=2011575.pdf ; en allemand uniquement).

Dans le canton de Zurich, le projet a été discuté dans le détail et rejeté. Le rapport final relatif à l'avant-projet sur la nécessité de réglementer la cyberadministration, qui étaie la décision du Conseil d'Etat, peut être consulté à l'adresse suivante : http://www.zh.ch/internet/de/aktuell/rrb/suche.html (numéro RRB 559 ; en allemand uniquement).

4.2 Mesures au niveau du projet

Chaque projet de cyberadministration doit, au final, fonctionner dans des conditions-cadre spécifiques. Il faut lever tous les obstacles subsistant encore et créer toutes les conditions manquantes, c'est-à-dire également les bases légales. Indépendamment du cadre légal concret, les projets de cyberadministration sont presque toujours très complexes. Leur réussite nécessite de grandes compétences, beaucoup d'habileté et un grand engagement.

S'agissant du cadre légal et des autres activités juridiques, quatre éléments essentiels à un travail de projet couronné de succès ont été identifiés :

- Garantir que l'équipe de projet possède des connaissances juridiques suffisantes
  Il convient de veiller dès le début à ce que l'équipe de projet possède des connaissances juridiques suffisantes. Pour ce faire, elle compte normalement un juriste, qui travaille à un pourcentage défini pour le projet. Le fait qu'un service juridique prenne occasionnellement position sur des

questions précises ou mette le doigt sur des problèmes, ne suffit pas.
De plus, il importerait de s'assurer que le service compétent en matière de protection des données est intégré le plus tôt possible dans le projet et qu'il formule des propositions concrètes.

- Confier le projet au service compétent
  On tiendra mieux compte de l'aspect ci-dessus si le service compétent sur le fond conserve la responsabilité du projet de cyberadministration et que celui-ci n'est pas repris par un service spécialisé dans l'informatique, l'organisation ou la cyberadministration. Le service compétent a, le plus souvent, une bonne connaissance des bases légales régissant son activité et des procédures à appliquer en cas d'adaptation.
- Inscrire l'élaboration de la base légale comme une tâche normale dans la planification
  Les tâches à accomplir dans le domaine juridique, comme la création d'une base légale, la suppression des prescriptions posant des obstacles ou le fait de demander une autorisation, ne doivent pas être gérées en dehors du projet, dans le cadre d'une planification séparée. La direction, le suivi et l'exécution de ces tâches doivent s'inscrire dans la planification globale du projet, comme c'est le cas pour les autres tâches. C'est le meilleur moyen de garantir que leur importance et leur influence sur la planification dans son ensemble sont visibles et qu'elles peuvent être prises en compte. Il faut, entre autres, tenir compte du temps nécessaire aux adaptations de la loi, lesquelles sont, en règle générale, du ressort des parlements cantonaux.
- Sécurité adaptée : solutions pragmatiques, pas d'équipement technique très perfectionné
  Lorsqu'une étape de la procédure est informatisée, il convient d'abord de réfléchir pour déterminer le niveau réel des besoins en termes de sécurité dans le cas concret. Les prescriptions de forme existantes ne doivent pas être reprises sans examen préalable. Celles-là ont fréquemment été rédigées à une époque où l'on ne pouvait choisir qu'entre la forme écrite ou pas de forme du tout. Des mesures de sécurité élevées, comme la signature électronique, ne doivent pas être exigées simplement parce qu'elles existent, mais uniquement car elles sont indispensables dans le cas concret. Dans la plupart des situations, un simple message électronique devrait, par exemple, suffire pour une opposition. En ce qui concerne les publications officielles, on ne voit pas, dans de nombreux cas, pourquoi la forme électronique ne suffirait pas.

4.3 Conditions pour d'autres mesures à l'échelon fédéral

Même si tous les participants entendent promouvoir la cyberadministration, les principes politiques et juridiques en vigueur, tels que le fédéralisme, le principe de la légalité et celui de proportionnalité, ne peuvent généralement pas être mis de côté. Pour changer la donne en faveur d'une règlementation fédérale de grande envergure, il faudrait tout d'abord élaborer les bases légales nécessaires à l'échelon de la Constitution et de la loi.

Même dans les domaines où la Constitution prévoit des compétences suffisamment étendues, par exemple le droit civil, le droit de la procédure civile ou les postes et télécommunications, il faut élaborer les bases nécessaires au niveau de la loi avant de pouvoir mettre en œuvre une règlementation plus concrète. C'est ce que permet l'art. 45a du code civil pour le registre de l'état civil informatisé Infostar.

Par ailleurs, il est évidemment possible d'élaborer, conjointement ou de manière harmonisée au moins, un règlement national non pas via la Confédération mais via un concordat de tous les cantons. Les conventions-cadre correspondantes permettraient, en particulier, de consolider, sur les plans contractuel et institutionnel, la mise en œuvre de l'organisation « E-Government Suisse ». On ouvrirait ainsi la voie à des développements communs, voire à des normes contraignantes en matière de réglementation, de procédures et d'applications informatiques.

Le chap. 5.2 – et en particulier l'avis de droit de l'OFJ qui y est mentionné [5] – fournit des explications sur les bases légales permettant à la Confédération et aux cantons de coopérer dans les domaines des technologies de l'information et de la communication.

Les modifications potentielles de la marge de manœuvre mentionnées ci-dessus peuvent, en grande partie, être opérées à moyen et long terme. En revanche, les mesures à l'échelon fédéral citées et recommandées ci-dessous (voir chap. 6) doivent pouvoir être mises en application en s'appuyant sur les conditions-cadre existantes.

5 Travaux achevés

Le sujet des bases légales pour la cyberadministration est traité depuis quelques années. Il est également abordé, comme nous l'avons expliqué en introduction, dans le contexte de la société de l'information. Aussi existe-t-il une série de projets déjà concrétisés ou mis en œuvre entre-temps qui visent à améliorer la situation dans ces deux domaines.

5.1 Développement dans le domaine de la communication électronique avec les autorités

L'entrée en vigueur au 1er janvier 2011 des deux nouveaux codes de procédure[6], l'obligation qui en découle pour les autorités de réceptionner les actes électroniques et l'entrée en force des deux ordonnances d'exécution – l'OCE-PA et l'OCE-PCPP – ont permis d'introduire un modèle de réglementation complet pour la communication électronique. Les cantons peuvent s'en inspirer pour leurs réglementations.

Le projet d'ordonnance sur l'acte authentique électronique[7] constitue un autre texte législatif modèle. [6]. Le projet présenté au chapitre 6.1.4 soutiendra la mise en œuvre de ce développement dans les cantons.

Enfin, un outil facilement accessible - la SuisseID – a été conçu, sous la houlette du SECO, et mis à la disposition des utilisateurs pour l'authentification sécurisée, la signature juridiquement valide et la preuve d'identité sécurisée. La SuisseID a également trouvé sa place dans la pratique du monde juridique étant donné qu'elle est intégrée dans la carte d'avocat émise par la Fédération suisse des avocats (FSA).

Conformément à l'art. 130, al. 2, CPC et à l'art. 110, al. 2, CPP, le Conseil fédéral détermine le format des documents transmis par voie électronique. Il faudra attendre qu'il soit possible de transmettre des données structurées pour constater de véritables gains d'efficacité auprès des autorités et des tribunaux (saisie automatique dans les systèmes internes). Les travaux préliminaires du projet JusLink ont déjà permis en grande partie de définir les formats des documents transmis par voie électronique. Avant de les appliquer, il est nécessaire de passer par une phase pilote pour les tester. Mais il n'y a pas de fonds prévus à cet effet.

En ce qui concerne la communication électronique et la signature numérique, il s'agira, à l'avenir, surtout de familiariser une large base de praticiens avec les techniques et de supprimer les malentendus et les incertitudes persistantes au moyen de mesures de formation et de soutien. Le train de mesures 3, transmission des connaissances, décrit ci-dessous doit couvrir ces activités.

---

[6] Code de procédure civile du 19 décembre 2008 (CPC, RS 272) et code de procédure pénale du 5 octobre 2007 (CPP, RS 312.0).

[7] Partie intégrante du projet de révision partielle des droits réels immobiliers et du droit du registre foncier (lien ci-dessous, au bas de la page) :
http://www.bj.admin.ch/content/bj/fr/home/themen/wirtschaft/gesetzgebung/abgeschlossene_projekte/immobiliarsachenrecht.html

5.2 Avis de droit et guides

1. Guide relatif aux bases légales pour le traitement de données personnelles

Comme nous l'avons mentionné plus haut, l'OFJ a élaboré et publié sur Internet, en 2010, un guide exhaustif pour l'élaboration des bases légales nécessaires pour exploiter un système de traitement automatisé de données personnelles (18 pages) [7].

2. Chapitre consacré au droit dans le manuel pratique de cyberadministration de mars 2009

Des indications et des explications exhaustives sur les questions juridiques qui se posent dans le cadre de la cyberadministration figurent en outre dans le chapitre 4.4 « Droit » de l'édition complétée du manuel pratique de la cyberadministration de l'USIC et de la direction opérationnelle d'E-Government Suisse, parue en mars 2009 [8].

3. Avis de droit de l'OFJ sur la coopération entre Confédération et cantons dans le domaine des technologies de l'information et de la communication

Le 6 juillet 2011, annonçant la mise en œuvre de sa stratégie sur la société de l'information, le Conseil fédéral a chargé le DFJP d'étudier avant la fin 2011 la question des bases légales nécessaires à une coopération entre la Confédération et les cantons dans le domaine des technologies de l'information et de la communication et de déterminer les adaptations législatives qui s'imposent.

Le 22 décembre 2011, l'OFJ lui a remis un avis de droit intitulé « Rechtsgrundlagen für die IKT-Zusammenarbeit zwischen dem Bund und den Kantonen » (uniquement en allemand) [5]. Le Conseil fédéral en a pris acte et l'a transmis à la direction opérationnelle d'eGovernment Suisse pour qu'il en soit discuté au sein du comité de pilotage. L'avis a été publié en mai 2012 dans la Jurisprudence des autorités administratives de la Confédération (JAAC).

L'avis contient pour l'essentiel les conclusions suivantes :

1. Il n'existe pas à l'heure actuelle de base constitutionnelle attribuant à la Confédération une compétence législative en matière de coopération avec les cantons dans le domaine des technologies de l'information et de la communication. Pour que la Confédération puisse imposer une cyberadministration unifiée, il faudrait commencer par créer une telle base constitutionnelle.
2. Il existe par contre des bases constitutionnelles dans divers sous-domaines : le droit civil, le droit de la procédure civile, le droit pénal, le droit de la procédure pénale et par ex. (art. 92, al. 1, Cst.) les postes et télécommunications.
3. Dans les domaines où la Constitution attribue une compétence globale à la Confédération, c'est-à-dire une compétence qui ne se limite pas à la fixation de principes, celle-ci peut régler les questions relatives à la coopération dans le domaine des technologies de l'information et de la communication, pour autant que ces règles servent à faire exécuter le droit fédéral et soient conformes au principe de la proportionnalité.
4. Même s'il y a une base constitutionnelle, la Confédération doit avant tout élaborer une législation d'application sous la forme d'une base légale formelle.
5. Elle peut aussi, en lieu et place d'une base légale formelle, conclure des conventions avec les cantons, comme elle l'a fait dans le cadre de la Conférence suisse sur l'informatique (CSI) s'agissant de la collaboration entre collectivités publiques suisses en matière d'informatique ou encore en signant la convention-cadre de droit public concernant la collaboration en matière de cyberadministration en Suisse, ou encourager l'adoption de normes volontaires ou de meilleures pratiques.

6 Trains de mesures proposés

Une fois les différentes délimitations effectuées, il reste à adopter des mesures permettant de compléter les bases légales de la cyberadministration et de répondre à certaines questions juridiques qui se posent dans ce contexte. Ces mesures sont réparties en trois trains, en fonction de leur caractère :

1. train de mesures 1 : législation
2. train de mesures 2 : infrastructures de base et composants d'une cyberadministration nationale
3. train de mesures 3 : transmission des connaissances

La réalisation d'une partie des mesures proposées a déjà été mandatée ou est en cours. Les mesures restantes doivent encore être préparées, c'est-à-dire qu'un département fédéral doit être nommé responsable de l'élaboration des étapes de mise en œuvre.

6.1 Train de mesures 1 : législation

Bien que la marge de manœuvre pour la création de bases légales à l'échelon fédéral soit plutôt réduite, il existe tout de même quelques domaines dans lesquels il est possible d'apporter des améliorations tant au niveau fédéral que dans d'autres domaines de la législation.

6.1.1 Perfectionnement de la signature électronique

La SCSE, qui régit la signature électronique, est entrée en vigueur en 2003. Entre-temps, deux générations de cartes-signature fondées sur cette loi ont été lancées sur le marché. Il convient maintenant de supprimer certaines lacunes et certains points faibles identifiés. Une reconnaissance des signatures au niveau international - en Europe au moins - et un positionnement juridique clair des certificats ou des signatures des serveurs et des entreprises font défaut jusqu'ici. Par ailleurs, il importe d'examiner si toute signature qualifiée ne devrait pas obligatoirement être assortie d'un horodatage reconnu.

Concrétisation : En vue de consolider les bases légales pour la société de l'information en Suisse (voir chap. 2), le Conseil fédéral a chargé le DFJP en juillet 2011 de rédiger un avant-projet prêt à être mis en consultation ainsi qu'un rapport explicatif sur ces questions et de le lui présenter d'ici le début de l'année 2012. Le Conseil fédéral a lancé la consultation le 28 mars 2012. Celle-ci durera jusqu'au début du mois de juillet 2012. Les résultats de la consultation seront dépouillés au cours du deuxième semestre 2012. Le message à l'intention du Parlement sera élaboré dans le même temps.

6.1.2 Perfectionnement de la communication électronique avec les autorités

Les dispositions relatives aux actes électroniques et à leur notification par voie électronique figurant dans les deux nouveaux codes de procédure et les deux ordonnances d'exécution (OCE-PA et OCE-PCPP) ont permis de franchir une première étape importante dans le domaine de la communication électronique avec les autorités.

Toutefois, il convient de poursuivre ce processus. Dans ce contexte, la Confédération et ses procédures doivent continuer de jouer un rôle pionnier, d'une part par l'intégration de la transmission de données structurées, d'autre part par l'ajout de nouveaux domaines dans lesquels il serait au moins possible de transmettre des documents par voie électronique et, enfin, par la mise en œuvre des procédures individuelles qui autoriseraient exclusivement la transmission électronique et la rendraient donc obligatoire pour tous les partenaires concernés, dans le cadre notamment de procédures relevant du droit fédéral (par ex. état civil, registre du commerce, armée, aviation et funiculaires). Il ne faut donc pas uniquement se pencher sur la communication entre des particuliers et les autorités, mais aussi et surtout sur la communication entre les autorités, au sein desquelles la procédure électronique devrait être introduite très rapidement.

Concrétisation : le DFJP prépare des instructions sur la transmission de données structurées dans le cadre des procédures relevant du CPC et du CPP, procède à un essai pilote et fait entrer les instructions en vigueur d'ici au début 2014.

Il dresse en outre un inventaire des procédures relevant du droit fédéral et de leur degré d'informatisation (actes électroniques et notification par voie électronique : impossibles/en partie possibles/possibles/obligatoires) et rédige, chaque année, un rapport actualisé sur la situation, à l'intention du comité de pilotage.

Autre forme de communication : le fait qu'outre la forme écrite, il n'existe, en Suisse, aucune forme de communication ayant une portée juridique définie, constitue un grand obstacle à la communication électronique. Vus sous cet angle, un document sans signature, un message électronique, un entretien et des signaux de fumée ont la même valeur. Seul le fax a obtenu une certaine reconnaissance, principalement dans la jurisprudence et, dans une moindre mesure, dans la doctrine. En d'autres termes, la signature électronique selon la SCSE est, pour la communication juridique, la forme minimale définie juridiquement. Il s'agit là d'un obstacle considérable. L'« absence de signification » sur le plan juridique de toutes les autres formes de communication contraste, en outre, avec la pratique quotidienne, où les messages électroniques revêtent une importance fondamentale. Même si la modification des prescriptions de forme touche des concepts fondamentaux, il conviendrait d'étudier la possibilité d'introduire une ou plusieurs formes de communication ayant un niveau d'exigences moindre que la forme écrite. La forme littérale (*Textform*) conformément au droit allemand (voir le § 126b du code civil allemand [BGB]) peut servir de modèle.

Concrétisation : le DFJP examine la possibilité d'introduire une ou plusieurs formes de communication qui, en comparaison avec la forme écrite, ne présentent pas des exigences aussi élevées. Il rédige une expertise à ce sujet d'ici le milieu de l'année 2013.

En outre, la ***transmission*** des communications tant entre autorités que dans l'économie privée nécessite d'être réglementée. La libéralisation dans le domaine du courrier postal a considérablement modifié les rapports ces dernières années. Toutefois, les notions juridiques n'ont, quant à elles, pas fait l'objet d'une adaptation suffisamment claire et significative. Des éléments importants de la transmission électronique, pertinents d'un point de vue juridique, comme la confidentialité, la confirmation de l'envoi et la délimitation des compétences ou de la responsabilité, doivent être réglés en intégrant les nouveaux acteurs.

Dans ce contexte, il importe également d'étudier s'il ne conviendrait pas d'introduire, en Suisse aussi, une réglementation se fondant sur l'exemple de l'Allemagne (« De-Mail »)[8] ou d'autres pays pour les services de messagerie électronique particulièrement dignes de confiance et de rendre ces services obligatoires dans certaines circonstances. Une telle réglementation pourrait voir le jour en lien avec la SuisseID ou la future carte d'identité.

Concrétisation : le DETEC élabore, d'ici le milieu de l'année 2013, une ébauche de projet pour une telle législation.

6.1.3 Normes et modèle de réglementation pour l'utilisation de plusieurs supports de données

La phase de transfert des procédures sur papier aux procédures électroniques bat son plein. Pendant cette période de transition, qui devrait durer encore 20 ou 30 ans, la communication sur papier et la communication électronique cohabiteront dans les échanges avec les autorités, ce qui rend nécessaire, dans de nombreux cas, le passage d'un support de données à un autre. Il est donc souhaitable de

[8] Voir la loi allemande du 28 avril 2011 sur la réglementation des services De-Mail et sur la modification d'autres prescriptions (*Gesetz zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften*).

pouvoir conserver les caractéristiques essentielles d'un document (par ex. les preuves) lors du passage d'un support de données à l'autre.

Au cours des prochaines années, tous les législateurs cantonaux et de nombreux organes responsables au sein de l'économie privée devront préparer des prescriptions afférant à l'utilisation de plusieurs supports de données. Par ailleurs, des centaines voire des milliers de personnes compétentes en matière d'enregistrement ou d'archivage de données, travaillant dans des entreprises privées ou des services publics devront les mettre en application dans la pratique. Dans ce contexte, la question se pose de savoir comment des normes et des directives permettraient de réglementer à l'échelle nationale, le plus efficacement et le plus uniformément possible, le passage de documents papier à des documents électroniques (P->E) et vice-versa (E->P). Si l'on parvient, dans les délais impartis, à mettre à disposition une base commune et utilisable pour la multitude de prescriptions et de solutions à venir, il en résultera une grande utilité pour tous les participants. On pourra ainsi éviter le foisonnement de solutions qui ne sont pas comparables entre elles, avoir une meilleure vue d'ensemble et coordonner la formation.

Concrétisation : le DFJP prépare, d'ici la mi-2012, une analyse de la situation ainsi qu'une conception générale de la réglementation exhaustive du passage d'un support de données à l'autre et le soumet à une large consultation.

6.1.4 Modèle de législation pour la mise en œuvre au niveau cantonal de l'acte authentique électronique

Dans le cadre de la procédure mentionnée au chapitre 5.1 visant à réglementer, à l'échelon fédéral, l'acte authentique électronique, les bases légales cantonales relatives à ce sujet sont actuellement évaluées en collaboration avec la Fédération suisse des notaires. Les besoins d'adaptation seront recensés dans ce cadre et des moyens auxiliaires pour les projets de réforme cantonaux mis au point.

Concrétisation : le DFJP élabore, conjointement avec la Fédération suisse des notaires, un guide de rédaction de la législation cantonale d'exécution relative à la mise en œuvre de l'acte authentique électronique et un modèle de loi.

6.2 Train de mesures 2 : Composants nationaux des infrastructures de base de la cyberadministration

Les projets réalisés dans le cadre de ce train de mesures ont mis l'accent sur les aspects organisationnels. La question de savoir s'ils aboutiront à un projet de loi et quelle sera la nature de celui-ci, demeure encore ouverte.

6.2.1 Conception d'un identificateur national de personnes

La décision d'introduire le nouveau numéro AVS (NAVS13), prise en 2004, a mis fin aux nombreuses années de débat sur un identificateur de personnes à grande échelle. Depuis 2007, des domaines choisis, notamment les assurances sociales, le registre des personnes, la formation et les impôts, disposent du NAVS13. La question d'une identification univoque des personnes et celle des identificateurs se posent, néanmoins, dans de nombreux autres secteurs de la cyberadministration (par ex. registre du commerce, registre foncier ou système de santé).

Ces dernières années, la Confédération et les cantons ont créé, pour certains autres domaines, des bases légales (conformément à l'art. 50*e* de la loi sur l'assurance-vieillesse et survivants) relatives à l'utilisation du NAVS13. Il en résulte une incertitude sur le fait que le NAVS13 puisse devenir un identificateur de personnes à grande échelle, sur les conditions auxquelles ce pourrait être le cas et sur les autres solutions existantes. Ces questions ont été formulées par divers milieux ces derniers mois. La Confédération doit les traiter et prendre une décision rapidement.

Concrétisation : il faut mettre au point une proposition de conception des identificateurs de personnes valables pour tous les domaines de la cyberadministration et pour les applications privées. Les compétences doivent être définies.

6.2.2 Conception de l'organisation et du financement des infrastructures de base nationales nécessaires à la cyberadministration

Compte tenu de l'intensité croissante des interactions entre les différentes autorités, il n'est pas judicieux d'exploiter, de manière décentralisée et multiple, les infrastructures de base, telles que les registres, les répertoires ou les services IAM. Mais il est rare qu'il existe un organe responsable acceptable pour tous les participants et susceptible de reprendre, avec compétence et équité, les fonctions principales en termes de finances, de conduite et d'exploitation.

L'OFJ travaille à la création et à la mise sur pied progressive d'une organisation de cette nature, laquelle exploiterait les registres dans son domaine de compétence. L'objectif de ce projet doit être étendu à toutes les infrastructures et à tous les services qu'il est préférable d'exploiter dans une architecture nationale de cyberadministration.

Il convient d'étudier dans le cadre d'une phase séparée au sein de ce projet si une base constitutionnelle devrait être créée pour la répartition des tâches et pour le financement des infrastructures nationales de la cyberadministration.

Concrétisation : le 12 juillet 2011, le Conseil fédéral a chargé le DFJP de lui présenter une conception de l'organisation et du financement des infrastructures de base nationales nécessaires à la cyberadministration.

6.2.3 Applications intercantonales standard d'E-Government Suisse

Il arrive très souvent que les cantons développent des applications bien qu'il en existe déjà dans d'autres cantons ou qu'ils mettent au point au même moment une application valable pour le même domaine. Les informaticiens et leurs supérieurs hiérarchiques estiment que ces développements sont fondés, car ils estiment que les exigences spécifiques du canton concerné ne peuvent être remplies de manière optimale qu'à l'aide d'une application propre à ce canton. D'un point de vue financier et à l'échelle nationale, il s'agit là de doublons très souvent inutiles. Il en apparaît régulièrement en dépit de la coordination opérée par E-Government Suisse, la CSI et d'autres organes.

L'idée ***d'applications intercantonales standard*** constituerait un instrument permettant d'exercer une certaine pression en faveur de l'utilisation multiple, de l'harmonisation et des développements communs. Les organes d'E-Government Suisse, et en particulier le comité de pilotage, pourraient transformer, selon une procédure prédéfinie et pour un domaine précis, des applications existantes ou en cours de préparation en « applications standard ». Dès qu'un domaine dispose d'une ou de plusieurs applications standard ou que celles-ci sont en cours de conception, aucun autre canton ne doit développer d'applications supplémentaires. Les dérogations à ce principe doivent être approuvées, dans le cadre d'une procédure prédéfinie, d'une part par les services hiérarchiques compétents du canton et, d'autre part, à la demande de celui-ci, par le comité de pilotage d'E-Government Suisse. Il va de soi qu'un instrument de cette nature ne peut être utilisé que si tous les cantons acceptent au préalable de s'y soumettre volontairement, en approuvant, par exemple, une clause correspondante dans la convention-cadre.

La Confédération utilise des instruments similaires dans le cadre de la coordination interdépartementale. L'Allemagne fait de même pour la coordination « justice/informatique » entre les *Länder*.

Concrétisation : le comité de pilotage veille à l'élaboration d'une conception des applications intercantonales standard et prend une décision à ce sujet d'ici le milieu de l'année 2013.

6.3 Train de mesures 3 : transmission des connaissances

L'évaluation des problèmes et des attentes a mis en lumière que les connaissances techniques nécessaires à une exécution efficace des tâches juridiques faisaient très souvent défaut ou que des réponses ou des solutions avaient déjà été développées, mais qu'elles n'étaient pas connues des acteurs du projet. C'est pourquoi la résolution des problèmes liés aux bases légales passe principalement par une meilleure transmission des connaissances.

Une plate-forme spécialisée, une offre de cours et, enfin, un centre de compétences permettront de transmettre les connaissances. Ces trois piliers sont décrits sommairement ci-dessous afin de déterminer s'ils sont suffisamment prometteurs pour être développés davantage et mis en œuvre.

6.3.1 Plate-forme de connaissances sur les bases légales de la cyberadministration

Une plate-forme de connaissances sur Internet peut, actuellement, sembler banale. Toutefois, les expériences révèlent qu'une offre de cette nature peut devenir un outil précieux pour un groupe spécialisé si les possibilités disponibles sont combinées et exploitées de manière optimale, que la structure est attrayante et que les mises à jour sont régulières.

Dans le cas qui nous intéresse, cette plate-forme pourrait contenir les éléments suivants :

- un *répertoire complet de tous les projets de cyberadministration*, y compris ceux qui ne sont pas prioritaires, fournissant des informations utiles sur chacun d'entre eux ;
- un *répertoire de toutes les bases légales* de la cyberadministration aux échelons national, cantonal et international (lois, ordonnances, concordats, etc.) ;
- des *projets* de loi, de contrat, de formulaire sur des sujets choisis ;
- un recueil exploitable d'*expertises, de directives et de mémentos* portant sur différents sujets relatifs à l'orientation méthodologique ou concrète ;
- un recueil de *synthèses sur des questions individuelles* (par ex. des FAQ) ;
- un *forum de discussion* (questions/réponses) avec participation entre autres de juristes spécialisés de l'OFJ, de l'USIC, du PFPDT, de l'OFCOM, des cantons et d'études d'avocats privées, garantie sur la durée ;
- un *wiki* sur la rédaction commune et/ou la maintenance et l'optimisation régulières des projets, des mémentos, etc.

Il est déterminant pour la plupart de ces offres d'être exploitées via une systématique orientée sur les praticiens et les problèmes. Cette systématique peut devenir, à moyen terme, un élément central. Elle reste à créer pour le thème des bases légales de la cyberadministration.

6.3.2 Centre de compétences pour les bases légales de la cyberadministration

Si un service s'occupe de mettre en place une plate-forme de cette nature et d'en effectuer la maintenance, il pourrait simultanément, avec des ressources en personnel plus importantes, œuvrer en tant que centre de compétences pour les bases légales de la cyberadministration et, ainsi, proposer quelques prestations supplémentaires, telles que :

- la rédaction d'avis de droit et de réponses à des questions ;
- l'établissement d'autres directives concernant des sujets actuels (par ex. directive relative au choix de la méthode de signature et d'authentification) ;
- la réalisation d'audits de projets et de systèmes ;
- éventuellement, la participation à des projets de cyberadministration, en qualité de spécialistes du droit.

Un centre de compétences de ce genre requiert une réserve minimale de ressources. Une autre solution consiste à répartir les tâches de manière coordonnée entre des juristes spécialisés actifs au sein des autorités ou du secteur privé ou en collaboration avec un institut universitaire.

6.3.3 Offres de formation sur les bases légales de la cyberadministration

Les participants ont déploré l'absence quasi complète d'offres de formation ayant trait à ce sujet. En se fondant sur les activités menées sur la plate-forme de connaissances et sur les expériences faites avec les requérants, le centre de compétences pourrait – conjointement avec un institut universitaire éventuellement – préparer des cours et organiser, occasionnellement, des séminaires ou des conférences sur des thèmes actuels.

6.3.4 Mise en œuvre, compétence

L'Unité de stratégie informatique de la Confédération USIC se voit confier la réalisation directe du train de mesures 3, en collaboration avec la direction opérationnelle d'E-Government Suisse. Elle crée le service chargé de la mise sur pied et de la maintenance de la banque de données contenant les connaissances indispensables.

Elle assume la responsabilité du centre de compétences pour les bases légales dans le domaine de la cyberadministration et travaille à sa mise en œuvre et à son exploitation, conjointement avec l'OFJ et l'Association eJustice.CH (anciennement ASDIJ).

A condition que les cantons prennent en charge la moitié du projet, le DFF demandera que le budget comprenne la création de cinq postes supplémentaires et un crédit annuel d'1 million de francs, à titre de contribution de la Confédération à la concrétisation de ce projet commun.

7 Autres étapes, mise en œuvre

Le présent document met un terme à la phase d'analyse et de recherche de solutions pour le projet B1.02. Les trois trains de mesures proposés, découlant de tous les ateliers et de toutes les analyses, enquêtes et réflexions, sont des mises en œuvre judicieuses et réalisables à l'échelle nationale. Il incombe désormais aux mandants, aux instances décisionnaires et aux départements mandatés de déterminer si la mise en œuvre de ces mesures doit être confiée à un service, faire l'objet d'un financement et être effectivement réalisée.

Liste des mandats de mise en œuvre présentés plus haut

N°	Chapitre	OCF	Mandat	Délai
	Train de mesures 1 : législation			
1.	6.1.1	DFJP	Mener et évaluer la procédure de consultation sur la révision de la SCSE ; préparer le message.	Fin 2012
2.	6.1.2	DFJP	Préparer des instructions sur la transmission de données structurées dans le cadre des procédures relevant du CPC et du CPP, procéder à un essai pilote et faire entrer les instructions en vigueur.	Début 2014
3.	6.1.2	DFJP	Dresser un inventaire des procédures relevant du droit fédéral et de leur degré d'informatisation (informatisation : impossible/possible/ obligatoire).	Début 2013
4.	6.1.2	DFJP	Rédiger une expertise sur la question de l'introduction d'une autre forme juridique, entre la forme écrite et l'absence de forme.	Milieu de l'année 2013
5.	6.1.2	DETEC	Elaborer une ébauche de projet pour une législation sur la notification électronique et pour les messages électroniques réglementés par l'Etat.	Milieu de l'année 2013
6.	6.1.3	DFJP	Faire une analyse de la situation et élaborer une conception générale de réglementation global de l'utilisation de plusieurs supports de données.	Milieu de l'année 2012
7.	6.1.4	DFJP	Mettre au point, en collaboration avec la Fédération suisse des notaires, un guide de rédaction de la législation cantonale sur la mise en œuvre de l'acte authentique électronique et un modèle de législation.	Fin 2012
	Train de mesures 2 : infrastructures de base nationales de la cyberadministration			
8.	6.2.1	Non défini	Elaborer une proposition de conception des identificateurs de personnes pour toutes les applications publiques et privées (en lien avec le mandat du Conseil fédéral du 12.7.2011 relatif à l'examen de la possibilité d'introduire un identificateur de personnes dans le domaine de la justice).	Non défini
9.	6.2.2	DFJP	Elaborer, conformément au mandat du Conseil fédéral de juillet 2011, une conception de l'organisation et du financement d'infrastructures de base nationales dans le domaine de la cyberadministration.	Milieu de l'année 2012
10.	6.2.3	eGov-CH	Elaborer une conception des applications intercantonales standard en vue d'une utilisation multiple imposée d'ici le printemps 2013 et prendre une décision à ce sujet d'ici le milieu de l'année 2013.	Milieu de l'année 2013

	Train de mesures 3 : transmission des connaissances			
11.	6.3.4	DFF	Mettre en application le train de mesures 3 (transmission des connaissances) en collaboration avec la direction opérationnelle d'E-Government Suisse.	
12.	6.3.4	DFF	Mettre en place, conjointement avec l'OFJ et l'Association eJustice, le centre de compétences des bases légales dans le domaine de la cyberadministration.	

Une fois la mise en œuvre décidée et la réalisation de chaque mesure d'exécution donnée en mandat conformément à la liste ci-dessus, il conviendra de choisir entre deux variantes:

A) Le projet B1.02 est maintenu, mais il passe de nouveau sous la houlette de la direction opérationnelle E-Government Suisse.

B) Le projet B1.02 est clos en tant que tel.
Le sujet demeure bien entendu d'actualité. Il importe de continuer de l'observer dans le cadre de la gestion de la cyberadministration et de le mettre occasionnellement à l'ordre du jour. Les mesures de mise en œuvre réalisées sous la forme de projets constituent les éléments restants. En fonction de l'évolution, la question des bases légales pourrait être réévaluée dans quelques années dans le cadre d'un nouveau mandat.

8 Annexes

I. B1.02 Bases légales : enquête sur la nécessité de légiférer - questionnaire

II. B1.02 Bases légales : enquête sur la nécessité de légiférer - évaluation

9 Bibliographie

[1] Office fédéral de la communication OFCOM, « Consolidation des bases légales – Rapport du groupe de travail interdépartemental sur les résultats du mandat d'examen », 2009.

[2] L. Fässler, «Resultate Workshop "Rechtsgrundlagen" – ffO-Workshop du 18 juin 2009,» egovernment schweiz suisse svizzera, 2009 (en allemand uniquement).

[3] E-Government Suisse, « Projet prioritaire B1.02 Bases légales : Enquête sur la nécessité de légiférer – questionnaire », http://www.fsdz.ch/cms/uploaded/file/Umfragebogen_f_Formular.pdf, 2011.

[4] E-Government Suisse, « *Projet prioritaire B1.02 Bases légales : Enquête sur la nécessité de légiférer – évaluation* », 2011.

[5] Office fédéral de la justice, « Rechtsgrundlagen für die IKT-Zusammenarbeit zwischen dem Bund und den Kantonen » (uniquement en allemand), *Jurisprudence des autorités administratives de la Confédération*, JAAC 2012, n°1, pp. 1 à 17, 1er mai 2012.

[6] Office fédéral de la justice, « Ordonnance sur l'acte authentique électronique (OAAE) », http://www.bj.admin.ch/content/dam/data/wirtschaft/gesetzgebung/immobiliarsachenrecht/entw-veoeb-f.pdf, 2010.

[7] Office fédéral de la justice, « Guide pour l'élaboration des bases légales nécessaires pour exploiter un système de traitement automatisé de données personnelles », 2010.

[8] Unité de stratégie informatique de la Confédération USIC, « Manuel pratique de cyberadminsitration - Marche à suivre pour le développement de prestations électroniques dans les administrations publiques », egovernment schweiz suisse svizzera, 2009.