Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Préposé fédéral à la protection des données et à la transparence
PFPDT

Convegno pubblico,
Bellinzona, venerdi 27 aprile 2012

« Vingt ans de législation sur la protection des données, rétrospectives et perspectives »

L'évolution du droit de la protection des données : perspectives

Jean-Philippe Walter, Dr en droit
Préposé fédéral suppléant

I. Introduction

Lorsque le 19 juin 1992, le Parlement helvétique a adopté la loi fédérale sur la protection des données, nous sortions de l'affaire des fiches et le paysage en matière de traitement des données personnelles était foncièrement différent d'aujourd'hui. Certes depuis quelques années, les premiers ordinateurs portables avaient fait leur apparition dans les Universités, les administrations et les entreprises. Toutefois, nous étions encore à l'heure des gros ordinateurs dans des centres de calcul localisés ou facilement localisables et l'informatique était le fait d'une certaine « élite ». En outre, un grand nombre de traitement se faisait de manière traditionnelle et les données étaient stockées sous forme papier dans des fichiers manuels. L'Internet ne fit son apparition que quelques années plus tard. On ne parlait alors pas encore d'informatique pour tous, de téléphone portable ou de tablette intelligente, ni de l'Internet des choses, de réseaux sociaux, de géo localisation, de nuage informatique ou de nanotechnologies. Aujourd'hui l'informatique s'est démocratisée, est à la portée de tous et est omniprésente, sans pour autant que les traitements de données ne soient plus transparents. Sans perdre ses dimensions centralisatrices, elle est devenue multifonctionnelle et ubiquiste. Chacun d'entre-nous possède au moins un ordinateur ou un téléphone portable. Le traitement des données prend d'autres formes et est le fait de nouveaux acteurs. L'individu est à la fois personne concernée par le traitement des données, mais également responsable d'un certain nombre de traitements qu'il effectue, notamment en ligne. Sans pour autant remettre en cause les principes de base du droit de la protection des données, il convient néanmoins d'envisager des réformes pour répondre de manière plus effective aux enjeux et risques pour les droits et les libertés fondamentales découlant des évolutions technologiques et sociétales auxquelles nous sommes confrontées.

II. Evaluation de la loi fédérale sur la protection des données

Estimant que la protection des données concernait un grand nombre de personnes et que les développements technologiques intervenus depuis l'adoption de la LPD étaient éventuellement insuffisamment pris en compte par la législation existante et qu'ils pouvaient entraîner de nouveaux risques

Feldeggweg 1, 3003 Berne
Tél. 031 323 74 84, Fax 031 325 99 96
www.edoeb.admin.ch

pour les personnes concernées, l'Office fédéral de la justice a, sur la base de l'article 170 de la Constitution fédérale, lancé une évaluation de la loi fédérale sur la protection des données.

L'évaluation a démarré au printemps 2010 et s'est terminé en février 2011. Elle a été conduite par une équipe interdisciplinaire composée du bureau Vatter AG à Berne, de l'Institut de droit européen de l'Université de Fribourg et de l'Institut DemoScope. Les évaluateurs étaient supervisés par l'Office fédéral de la justice et un groupe de travail composé de représentants de l'administration fédérale, d'universitaires, de représentants de l'économie, d'un avocat, d'un représentant de Privatim et d'un représentant du PFPDT. L'évaluation a débouché sur un volumineux rapport[1] sur la base duquel le Conseil fédéral a rédigé un rapport du Conseil fédéral à l'adresse des Chambres fédérales[2].

L'objectif de l'évaluation était d'analyser l'effectivité et l'efficacité de certaines dispositions de la loi, le cas échéant de faire des propositions de modification. Pour des raisons financières, l'évaluation s'est focalisée sur certains aspects de la loi. Elle n'a également pas pris en compte les effets des dispositions introduites dans les révisions de la LPD entrées en vigueur le 1er janvier 2008 et le 1e décembre 2010. L'évaluation a mis l'accent principalement sur la connaissance de la loi et sur les mécanismes de mise en œuvre. En particulier les évaluateurs ont examiné dans quelle mesure les droits des personnes concernées et la procédure pour faire valoir ces droits permettent effectivement et de manière adéquate de garantir les droits et les libertés fondamentales, notamment le respect de la vie privée. Elle a également porté sur le rôle, les tâches et les compétences du Préposé fédéral à la protection des données et à la transparence.

L'évaluation montre que d'une manière générale la LPD permet en soi d'atteindre les objectifs visés. Elle débouche cependant sur un constat – qui ne surprend pas – selon lequel les menaces qui pèsent sur le respect des droits et des libertés fondamentales lors du traitement de données personnelles se sont renforcées ces dernières années. Les individus ont toujours plus de peine à conserver la maîtrise sur les données qui les concernent. L'évolution technologique et le volume de données qu'elle engendre sont des défis considérables non seulement pour les individus, mais aussi pour les responsables de traitement et les autorités de protection des données. Ainsi les évaluateurs reconnaissent que si le préposé fédéral remplit son mandat légal avec un haut degré d'efficacité, il rencontre néanmoins « des difficultés croissantes à exercer son mandat de surveillance étant donné l'accroissement constant de la fréquence, de l'opacité et de l'internationalisation des traitements. ». Ils relèvent un déficit au niveau de l'exercice des droits des personnes concernées. Ce déficit découle notamment du fait du coût et de la longueur des procédures. Il provient également du fait de l'importance et l'ampleur des données collectées quotidiennement et du fait que trop souvent les personnes ne prennent pas suffisamment conscience que des données sont collectées et traitées à leur égard.

Le Conseil fédéral dans le rapport qu'il a adressé au Parlement convient que la loi sur la protection des données doit être adaptée « aux rapides développements technologiques et sociétaux intervenus depuis son entrée en vigueur » et « prendre en compte les nouvelles menaces. » Il a donné mandat au DFJP de faire des propositions d'ici 2014. Il s'agit en particulier d'examiner quelles mesures permettraient : «

- D'assurer la protection des données plus en amont : une réflexion globale doit permettre de détecter les éventuels problèmes et d'y remédier dès la phase de conception des nouvelles technologies… Il importe de favoriser les technologies respectueuses de la protection des données.

[1] Disponible auprès de l'Office fédéral de la justice
[2] FF 2012, 255

- Sensibiliser davantage les personnes concernées : les personnes concernées doivent être plus au fait des risques que représentent les nouvelles technologies pour la protection de la personnalité
- Améliorer la transparence…
- Améliorer le contrôle et la maîtrise des données : le contrôle et la maîtrise des données après leur divulgation est un aspect primordial. Ainsi, la possibilité de renforcer les mécanismes de contrôle à disposition du PFPDT et d'adapter aux développements technologiques les droits des personnes concernées devrait être analysée. On examinera par exemple dans ce cadre un renforcement des voies de droit collectives ainsi qu'une précision du droit à l'oubli.
- Protéger les mineurs : il faut tenir compte du fait que les mineurs ont une conscience moindre des risques et conséquences inhérents au traitement de données à caractère personnel. »

Ce travail de mise à jour et de révision de notre droit de la protection des données devra tenir compte des travaux en cours au sein de l'Union européenne en vue d'un nouveau cadre juridique de protection des données et au Conseil de l'Europe avec la révision de la Convention 108. Le Conseil fédéral souhaite également examiner la répartition des compétences entre la Confédération et les cantons en matière de législation et de mise en œuvre, ainsi qu'un renforcement éventuel de l'indépendance du PFPDT et à l'introduction de mesures d'autoréglementation.

Parallèlement à l'évaluation de la LPD, deux postulats ont été déposés au Parlement. Tout d'abord le postulat 10.3383 d'Antonio Hodgers du 08.06.2010 « Adapter la loi sur la protection des données aux nouvelles technologies » demandant un renforcement du droit à la protection des données, notamment en introduisant une procédure de contrôle préalable, l'obligation d'intégrer les exigences de protection des données dans les systèmes et des audits externes. Le Conseil fédéral a accepté ce postulat. Ensuite le postulat 10.3651 de Jean-Pierre Graber du 14.09.2010 « Atteintes à la sphère privée et menaces indirectes sur les libertés individuelles » s'inquiétant de l'impact des technologies de surveillance sur la vie privée et demandant d'examiner la nécessité de renforcer de la légis-lation. Le Conseil fédéral propose également d'accepter ce postulat. En outre, le Conseil fédéral propose d'adopter un autre postulat 12.3152 déposé par Jean-Christophe Schwaab et qui demande en particulier d'examiner « l'opportunité d'ancrer et/ou de préciser dans la législation un droit à l'oubli numérique, en particulier en ce qui concerne les réseaux sociaux et les moteurs de recherche sur internet. »

III. Vers une révision de la loi fédérale sur la protection des données

La Suisse n'échappera ainsi pas au mouvement de mise à jour ou de modernisation de son droit de la protection des données. Le calendrier risque d'être dicté par les réformes au sein de l'Union européenne[3] et au Conseil de l'Europe[4]. Il ne faut cependant pas être attentiste, mais dès à présent entamer des réflexions de fonds et ne pas avoir peur d'une révision complète de notre droit et de notre organisation de la protection des données. Les autorités de protection des données doivent s'engager fermement dans le débat et le faire - autant que faire se peut – de manière coordonnée et uniforme. L'objectif doit cependant être clair : ne pas affaiblir l'acquis, mais rendre notre législation plus effective au bénéfice des droits et des libertés fondamentales touchés par le traitement de données personnelles. Si nous voulons favoriser le recours aux technologies de l'information et des

[3] Voir les propositions de commission européenne pour un nouveau cadre juridique européen de protection des données, http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

[4] Voir les travaux de modernisation de la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_fr.asp

communications, encourager l'innovation et bénéficier des avantages notamment sociaux, scientifiques, culturels, économiques qu'elles apportent aux individus et à la société, il est important de créer les conditions nécessaires à ce que chacun et chacune d'entre-nous puissent y recourir en toute confiance. La réussite de la société numérique passe obligatoirement par un haut niveau de protection des données.

Ici, je me limite à des considérations concernant principalement la loi fédérale. Sans remettre en question les fondements de la LPD, je suis d'avis que des aménagements sont nécessaires d'une part pour permettre une meilleure harmonisation avec le droit européen et ainsi mieux répondre aux attentes des entreprises actives sur le plan international et offrir le même niveau de protection des données aux personnes concernées. Cela est également nécessaire pour répondre aux nouveaux défis technologiques et à la dimension transfrontière et globalisée de l'information. Le traitement des données ne s'arrêtent pas aux frontières nationales ; il est dans notre intérêt d'élever le degré d'harmonisation de notre droit avec notre environnement immédiat pour garantir de manière efficace et effective le droit à la protection des données personnelles.

1. Objet et champ d'application

Actuellement, la LPD couvre l'ensemble des traitements de données personnelles, quels que soient leur nature et leurs modalités. Elle suit une approche dite technologiquement neutre, c.à.d. qu'elle ne règle pas spécifiquement le recours à telle ou telle technologie. Cette approche se doit d'être maintenue, même s'il est souhaitable de prévoir des règles particulières par rapport à certaines technologies ou type de traitements particulièrement invasifs.

Le champ d'application de la loi devrait être plus large et englober l'ensemble des traitements à l'exception des traitements dits domestiques. Des exceptions à certaines dispositions de la loi, notamment information, droit d'accès ou contrôle par le PFPDT devraient, autant que nécessaire être aménagées pour les traitements effectués dans le cadre de procédures judiciaires pendantes.

Les différences existantes dans le régime de protection des données des secteurs publics et privés doivent également être aplanies afin que les exigences de protection des données et le niveau de protection pour les individus soient les mêmes indépendamment que les données soient traitées par une personne privée ou qu'elles le soient par un organe fédéral. Cela aura des conséquences sur la structure de la loi.

Si au niveau de l'exécution et du contrôle, l'autonomie cantonale doit être préservée avec certains aménagements, la question de l'extension de l'application de la loi fédérale aux cantons doit être débattue. En effet, il me semble que les personnes sujet du traitement de données personnelles et la cohérence juridique y gagneraient si à l'instar de ce qui se prépare en Europe, nous uniformisions notre droit matériel de la protection des données en adoptant une loi cadre pour l'ensemble du pays avec éventuellement la possibilité pour les cantons d'adopter des lois d'application tenant compte au besoin des spécificités régionales. Cela passe nécessairement par une modification de la Constitution. Cette modification permettrait également de préciser le droit à la protection des données ancré à l'article 13 Cst.

2. Définitions

Les définitions doivent subir un toilettage et être adaptées, pour une question notamment de cohérence, au vocabulaire du droit européen et en particulier à celui de la Convention 108. Ainsi, la notion de maître de fichier devrait être remplacée par celle de responsable de traitement et complétée par celle

de sous-traitant. D'autres définitions, dans la mesure nécessaire, pourraient être introduites. Ces adaptations ou compléments doivent se faire de manière à ne pas affecter la sécurité du droit.

3. Principes de base de la protection des données

Les principes de base de la protection des données, tels qu'ils sont énoncés aux articles 4 et suivants LPD constituent le noyau dur de la protection des données. Il s'agit des principes de licéité, bonne foi, proportionnalité, finalité, exactitude des données et sécurité des données. Même si une plus grande convergence avec le cadre juridique européen nécessite une refonte de ces principes, leur essence ne doit pas être remise en question. Ils doivent néanmoins être complétés et renforcés en inscrivant dans la loi notamment le principe de la minimisation des données. Il s'agit en particulier d'éviter que des données personnelles soient collectées et traitées sous une forme identifiant la personne lorsque cela n'est pas nécessaire à la finalité du traitement. Ainsi l'offre de services anonymes ou permettant l'usage de pseudonyme doit être développée. Il faut également favoriser la création de systèmes de gestion des identités conforme à la protection des données, par exemple par le recours à des procédures anonymes ou sous pseudonymes et par la conservation décentralisée des données d'identification assurant un contrôle aussi large que possible par la personne concernée.

4. Droits des personnes concernées

La complexité des traitements de données, l'opacité grandissante qui les entoure, notamment lors du recours à des services en ligne ou dans les réseaux sociaux, la dispersion des informations au travers du nuage numérique ou encore la multiplication des acteurs ayant accès à l'information affaiblissent la position des personnes concernées et leur possibilité de faire valoir leurs droits. Une refonte du droit de la protection des donnés passe par un renforcement et un réaménagement des droits des personnes concernées qui doivent pouvoir se réattribuer la maîtrise sur les données qui les concernent. En effet, l'un des grands défis de l'Internet et du monde virtuel a trait à la gestion et à la maîtrise que nous pouvons avoir sur les données qui nous concernent. Une fois en ligne, l'information demeure et peut faire l'objet de traitements multiples et infinis dans des contextes différents, pour des finalités diverses et souvent pas compatibles entre elles ; ces traitements peuvent également être le fait d'acteurs différents. Toutes les actions de l'internaute peuvent être répertoriées et tracées quelle que soit sa position. Il est dès lors fondamental que les personnes concernées puissent bénéficier des mêmes droits que dans le monde réel et que leur exercice soit rendu aisément possible également en ligne.

4.1. Transparence

Il s'agit tout d'abord de renforcer la transparence des traitements en prévoyant l'information des personnes concernées de la collecte de données quel que soit la nature des données traitées et quel que soit l'organe, la personne ou l'entité qui procède à la collecte de ces données. L'information doit être aussi complète que possible et aisément accessible pour permettre aux individus de faire valoir leur droit et d'agir en connaissance de cause. L'information se doit être délivrée de manière intelligible et en des termes clairs et simples, adaptés aux publics cibles. On n'informera pas de la même manière un enfant qu'un adulte.

4.2. Droit d'accès

Le droit d'accès des personnes concernées doit être renforcé et porter également sur les aspects liés au profilage des individus et à la prise de décision automatisé. Son exercice devrait être simplifié et notamment pouvoir intervenir en ligne.

4.3. Droit à l'oubli

Le droit à l'oubli devra également être considéré, non dans l'idée de consacrer nécessairement un nouveau droit, mais plutôt de préciser ou de renforcer les droits existants en relation avec le droit d'opposition, y compris au profilage et aux activités de démarchage et de publicité, les droits de rectification et d'effacement des données et les obligations de conservation limitée des données. Il convient en effet de pouvoir garantir dans le monde virtuel les mêmes droits que dans le monde réel en rappelant l'existence du droit à l'oubli également dans les réseaux et en mettant en place des outils et des procédures propre à garantir ces droits, par exemple l'introduction d'une date de péremption des données et d'une obligation de désindexation des données. Il s'agira également d'adapter les modalités de l'exercice de ces droits de manière à le rendre plus aisé qu'actuellement.

4.4. Droit de portabilité des données

Le catalogue des droits doit être par contre complété par le droit de portabilité des données, selon lequel une personne a le droit d'obtenir du responsable du traitement une copie des données qu'il traite de manière automatisée dans un format électronique structuré couramment utilisé et qui permet la réutilisation des données par la personne concernée. Ce droit vise plus spécialement les données collectées par les fournisseurs de service Internet et doit permettre à la personne concernée, dans le respect de ses obligations notamment contractuelles, de transmettre ces données à un autre fournisseur ou opérateur.

4.5. Décisions automatisées

Enfin du fait que de plus en plus de décisions ou de mesures touchant les personnes concernées sont prises de manière automatisée, notamment sur la base d'activités de profilage, la loi doit aménager un droit de regard des personnes sur les décisions automatisées, en particulier celles qui ont des effets négatifs, leur permettant le cas échéant de contester la décision et de pouvoir faire valoir leur point de vue, voire de s'y opposer. D'autres droits pourraient également être envisagés, tel que le droit de s'opposer à la publication ou à l'indexation des données sur Internet, au droit de surfer sans être observé et profilé.

4.6. Recours et prétentions

En cas de non respect des droits des personnes concernées ou de conflits avec le responsable de traitement, l'accès aux autorités ou aux tribunaux devrait être repensé. En effet, l'un des graves déficits de notre système juridique a trait à la complexité et au coût des procédures. L'évaluation de la LPD l'a confirmé, les personnes concernées hésitent à agir en justice en cas de violation de leurs droits. Ainsi, il faudrait examiner la possibilité de procédures gratuites, d'introduire un droit d'action des associations ou d'envisager d'autres mécanismes de résolution des conflits, comme la médiation. Il conviendrait également d'examiner la possibilité d'introduire dans notre droit une véritable responsabilité objective du fait du traitement, la difficulté étant pour la personne concernée de démontrer qu'elle a subi un dommage. Il devrait ainsi revenir au responsable de traitement de prouver qu'il a agi conformément à la loi.

5. Obligation des « responsables » de traitement

Aujourd'hui notre loi contient quelques obligations spécifiques du maître de fichier ou responsable de traitement. Il est de manière générale responsable de respecter la loi. Il doit en outre assurer la trans-

parence des traitements et notamment informer les personnes concernées lors de la collecte de données, garantir les droits des personnes concernées, déclarer, dans la mesure où il n'est pas au bénéfice d'une exception, les fichiers de données personnelles qu'il détient, annoncer les mesures prises pour le transfert de données vers de pays n'assurant pas un niveau de protection des données adéquats et veiller à ce que le sous-traitant, lorsqu'il y recourt, assure la sécurité des données. Il est cependant nécessaire de compléter les obligations de ceux et celles qui traitent ou font traiter des données. En effet la garantie du droit à l'autodétermination informationnelle dépend aussi de la manière dont les responsables de traitement appliquent effectivement les dispositions de protection des données. Or, la détermination des mesures à prendre ne peut être laissée à la seule initiative des responsables de traitement ou de ceux et celles qui développent et/ou mettent à disposition des infrastructures de traitement, des services ou des technologies. Il incombe au législateur de fixer le cadre.

5.1. Privacy by design

Dans le cadre des travaux de révision, il conviendra de revoir le rôle des différents acteurs impliqués dans le traitement des données et en particulier celui des responsables de traitement et d'en préciser les obligations, notamment en vue d'améliorer la confiance des personnes dans les systèmes de traitement des données. Ainsi, il devrait être obligatoire de prendre en compte les principes de la protection des données dans l'organisation et dans le développement des systèmes d'information (principe du privacy by design et de la protection des données par défaut). Il est important en effet que les exigences de la protection des données soient prises en compte dès la conception des systèmes d'information et des technologies afin d'éviter la collecte et le traitement de données superflues, de limiter la conservation de ces données au minimum nécessaire et d'offrir aux personnes concernées une meilleure maîtrise sur leurs données, en évitant notamment que les données soient rendues accessibles à un nombre indéterminé de personnes.

5.2. Evaluation d'impact

D'autres mesures doivent être envisagées en fonction de l'importance et de la sensibilité des traitements de données, notamment l'obligation de procéder à une évaluation des risques d'atteinte au droit à la protection des données et à la vie privée, à des études d'impact sur la vie privée, par le biais de la certification fondés en particulier sur des audits externes agréés de protection des données.

5.3. Chargé de la protection des données

De même, l'instauration de chargés de la protection des données au sein des entreprises et des administrations devrait être généralisée et non pas reposer, comme actuellement, sur une norme incitative. Ces chargés de la protection des données devraient être des personnes de référence pour les autorités de protection des données.

5.4. Mesures techniques et organisationnelles

Une obligation d'annoncer les violations de données personnelles devrait être envisagée au moins dans les cas graves. Enfin, les conditions de recours à des sous-traitants, notamment quant aux garanties qu'ils doivent offrir en matière de respect de la protection des données devront être énoncées dans la loi. Le responsable de traitement ou le sous-traitant se doit également de documenter les différentes opérations de traitements qu'il effectue et de coopérer avec les autorités de contrôle, notamment pour leur démontrer les mesures prises pour respecter les exigences légales. Cette documentation devrait en particulier contenir une liste des traitements et des fichiers gérés par le responsable de traitement, indiquant notamment la finalité du traitement, les catégories de données traitées, les desti-

nataires ou catégories de destinataires des données, les modalités d'exercice des droits des personnes concernées (en particulier la personne ou l'organe responsable du droit d'accès). Cette liste devrait être à la disposition de l'autorité de protection des données compétentes et des personnes concernées. Ce renforcement des obligations du responsable de traitement, couplé à l'obligation de transparence des traitements permettrait de renoncer à l'obligation d'annoncer des fichiers au PFPDT.

5.5. Notification des traitements à risque élevé

Par contre comme le prévoit le postulat d'Antonio Hodgers du 8 juin 2010 et accepté par le Conseil fédéral, la LPD devrait prévoir une procédure de contrôle préalable par le PFPDT complétant l'objectif d'intégrer les exigences de la protection des données dans les systèmes de traitement des données, pour des traitements présentant un risque élevé d'atteinte aux droits et libertés fondamentales. Il s'agit en particulier des traitements de données sensibles ou de profils de la personnalité, des systèmes recourant à des technologies de surveillance des personnes (biométrie, vidéosurveillance, géolocalisation, RFID), des systèmes permettant le profilage des personnes ou permettant la collecte de données personnelles dans le cadre de service en ligne, de l'interconnexion des données provenant des fichiers ou de traitements gérés par des personnes ou organes publics différents ou encore des systèmes recourant à des traitements susceptibles, du fait de leur nature, de leur portée ou de leur finalité, d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat en l'absence de toute disposition légale (en particulier recours à des décisions automatisées).

5.6. Autres obligations

Si le responsable de traitement n'est pas établi en Suisse ou dans un pays assurant un niveau de protection adéquat reconnu, il devrait désigner un représentant en Suisse dès lors qu'il traite des données en Suisse ou qu'il offre régulièrement des biens ou des services à des personnes concernées domiciliées en Suisse.

Enfin notamment dans l'optique des transferts de données à l'étranger, il faut envisager d'encourager l'établissement de code de conduite en application de la LPD, de règles internes d'entreprises ou d'autres formes d'autoréglementation. Ces règles internes devraient faire l'objet d'une procédure d'approbation par le PFPDT ou de reconnaissance lorsqu'elles émanent d'entreprises sises hors de la Suisse et qu'elles ont été approuvées par une autre autorité de protection des données.

6. Surveillance

L'effectivité de la protection des données passe par l'existence d'autorité de surveillance, tel le préposé fédéral à la protection des données et à la transparence ou les autorités cantonales de protection des données.

6.1. Tâches et compétences

Ces autorités doivent comme actuellement exercer des tâches d'information, de sensibilisation, de conseil et de surveillance. Elles doivent pouvoir continuer à émettre des avis notamment sur les projets législatifs touchant à la protection des données. Elles doivent être dotées de pouvoirs d'intervention et d'investigation suffisants pour permettre une bonne application des lois de protection des données. Cela suppose que nos lois soient complétées ou précisées pour renforcer l'effectivité de ces pouvoirs. Ainsi, les autorités doivent avoir un pouvoir réel de mener des enquêtes et de prendre les mesures conservatoires nécessaires. Dans ce cadre, elles doivent pouvoir accéder aux locaux et installations de traitement des données, ainsi qu'aux traitements de données personnelles. Elles doi-

vent être dotées de pouvoirs de décision, notamment en vue de l'approbation de certains traitements à risque et le cas échéant pouvoir prononcer des sanctions dissuasives en cas de violation de la loi, lesquelles font actuellement défaut dans notre législation. Elles doivent également pouvoir agir en justice non seulement pour porter devant les tribunaux compétents les décisions ou recommandations qu'elles arrêtent lorsqu'elles sont contestées ou pas suivies d'effet, mais également contre des décisions d'autorités susceptibles de recours touchant de manière importante à la protection des données (par exemple risque d'atteinte grave aux droits d'un grand nombre de personnes).

6.2. Indépendance

L'existence d'une autorité de surveillance exerçant ses fonctions en toute indépendance est une composante essentielle de la protection des personnes lors du traitement de données personnelles. Cette indépendance est souvent objet de tension du fait notamment qu'elle est encore insuffisamment reflétée dans nos lois. L'indépendance se doit être :

- Institutionnelle : l'autorité de surveillance ne doit pas être subordonnée à une autre autorité gouvernementale. Cela exclut toute dépendance de l'autorité de surveillance et possibilité d'instructions émanant des autres autorités. Seuls les tribunaux sont habilités à revoir les décisions de l'autorité de surveillance. Toute influence extérieure sur les délibérations et les procédures menées par l'autorité doit être exclue. Cela implique aussi que les membres de l'autorité doivent s'abstenir de toute action ou fonction incompatible avec leurs tâches. Même si cela n'a pas jusqu'à ce jour poser de problèmes de conflits d'intérêts au niveau fédéral, les membres de l'autorité ne devraient pas exercer d'autres fonctions rétribuées durant la durée de leur mandat.
- Fonctionnelle : l'autorité n'est pas soumise à des interventions externes directes ou indirectes de tiers en relation avec le contenu et l'étendue de leurs activités. Les membres de l'autorité ne doivent pas pouvoir être démis de leur fonction du fait des opinions et des actions qu'ils sont appelés à émettre ou à entreprendre dans l'exercice de leurs tâches.
- Matérielle : l'autorité doit disposer de l'infrastructure nécessaire à l'accomplissement sans obstacle de ses tâches. Elle doit en particulier disposer d'un financement nécessaire adéquat. Le budget doit lui permettre d'avoir son propre personnel, ses locaux et de financer ses différentes activités nécessaires à l'accomplissement de ses tâches légales. Elle ne doit pas être soumise à un contrôle de ses dépenses qui puissent affecter son indépendance. Ainsi, il devrait pouvoir présenter son budget au gouvernement sans l'intervention d'intermédiaire et le défendre devant le parlement. Quant au financement de l'autorité, si actuellement il provient du budget global, d'autres pistes devraient à l'avenir être examinées et notamment la possibilité de financer partiellement ou totalement l'autorité en prélevant une taxe modeste auprès des personnes et des organes publics qui traitent des données personnelles, taxe tenant compte de la grandeur de l'entreprise, du volume de données traitées ou encore de la sensibilité des traitements.

6.3. Coopération

Les traitements de données personnelles sont de plus en plus globalisés et complexes. Ils impliquent différents acteurs et peuvent relever de différentes juridictions. La coopération entre autorités est ainsi indispensable et incontournable pour assurer une meilleure effectivité et efficacité dans l'accomplissement de leurs tâches. Elle doit également être mieux institutionnalisée dans nos lois pour permettre notamment aux autorités de partager des informations entre elles, de fournir une assistance mutuelle, de veiller à une application cohérente des dispositions légales ou de mener des

activités de contrôle conjointes et coordonnées et pour ce faire se doter d'une structure institutionnelle de collaboration.

Ainsi, les travaux de révision de la LPD doivent aussi permettre une réflexion sur l'organisation de la protection des données en Suisse dans le futur. Est-il encore raisonnable d'avoir au côté de l'autorité fédérale, des autorités cantonales de protection des données dans presque tous les cantons, dont certaines sont très largement sous dotées et dans l'impossibilité d'exercer effectivement leurs tâches ? Ne doit-on pas envisager un modèle différent qui passe par un regroupement des autorités de différents cantons à l'instar de Schwyz, Obwald et Nidwald ou de Neuchâtel et Jura ou opter pour la création de 3 ou 4 régions ? Je ne crois par contre pas, comme certaines autorités cantonales l'ont proposé, qu'il faille déléguer aux cantons les compétences du préposé fédéral à la protection des données et à la transparence dans le secteur privé. Cela irait à l'encontre des efforts en cours, notamment au niveau européen, d'assurer une plus grande cohérence et uniformité dans l'application du droit. Face à la globalisation et à l'internationalisation croissante des traitements, cela ne servirait pas les intérêts du secteur privé qui aspire à une simplification du système et à une diminution des intervenants dans la surveillance en matière de protection des données. L'argument de proximité des citoyens et citoyennes est certes important, mais pas déterminant dans un pays de la grandeur de la Suisse, notamment à l'heure où les technologies de l'information et des communications sont appelées à jouer un rôle croissant pour faciliter les démarches et les contacts avec les autorités. Nous courrons aussi le risque de voir certains responsables de traitement choisir pour siège des cantons où les autorités de protection des données seraient insuffisamment dotées.

IV. Conclusion

La loi fédérale sur la protection des données adoptée le 16 juin 1992 demeure certes une bonne loi et les principes qu'elles énoncent sont toujours pertinents au regard des développements technologiques intervenus depuis son adoption. L'approche technologiquement neutre et le cadre général de la loi doivent être maintenus. Toutefois, la loi doit être revisitée et complétée pour assurer une meilleure effectivité du respect du droit à la protection des données et permettre aux personnes d'avoir ou de retrouver la maîtrise sur les données qui les concernent. Cela passe par un renforcement des droits de personnes concernées, le développement des obligations des responsables de traitement et un renforcement des compétences et de l'indépendance de l'autorité de protection des données. Dans ce cadre, l'organisation des autorités suisses de protection des données doit être revue en particulier pour améliorer l'effectivité, la coopération et la coordination. Enfin, la lisibilité du droit fédéral de la protection des données et de la transparence y gagnerait en regroupant dans un texte les dispositions générales et sectorielles régissant la protection des données et la transparence (code le la protection des données et de l'accès aux documents officiels). Ce chantier de mise à jour doit débuter sans attendre tout en tenant compte du calendrier européen pour que notre législation soit également cohérente avec le droit européen de la protection des données (Convention du Conseil de l'Europe et cadre juridique de l'Union européenne).