La protection des données en Suisse

Autor(en): **Zellweger, Marie-Ange**

Objekttyp: **Article**

Zeitschrift: **Revue économique franco-suisse**

Band (Jahr): **75 (1995)**

Heft 1

PDF erstellt am: **17.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-886512

La protection des données en Suisse

Marie-Ange Zellweger, Avocat, Etude Zellweger et associés, La Neuveville

La loi fédérale suisse sur la protection des données (LPD) du 19 juin 1992 est entrée en vigueur le 1er juillet 1993. Son objectif : favoriser les échanges internationaux d'informations. Arrivée assez tardivement dans l'ordre juridique helvétique, cette loi a pour but de favoriser les échanges internationaux d'informations en rendant applicables en Suisse nombre de principes consacrés par le droit international public.

Un même texte régit les dispositions applicables au domaine privé et au secteur public et s'applique également aux personnes privées et aux personnes morales, c'est-à-dire particulièrement aux sociétés commerciales.

Le traitement de données personnelles ne peut s'effectuer que dans la mesure où les droits fondamentaux sont protégés (Message du Conseil Fédéral du 23 mars 1988, Feuille Fédérale n° 32). Le législateur a expressément rattaché ce droit à la liberté personnelle et à la protection de la personnalité, et non au droit de la propriété. Chacun, choisissant - en partie - son comportement personnel, doit intervenir en tant que sujet dans le processus de traitement des données le concernant. C'est le « **droit à l'autodétermination individuelle en matière d'information** ».

Dans ces conditions, la loi s'articule autour de trois axes :

- Elle détermine à quelles conditions des données personnelles peuvent être traitées et à quelles conditions des limites peuvent être apportées au droit à l'information.
- Elle assure la transparence du système par la publicité des fichiers et des traitements en accordant un droit d'accès à chaque personne.
- Elle met en place une structure de contrôle administratif et judiciaire.

LES SEPT PRINCIPES RÉGISSANT LE TRAITEMENT DES DONNÉES

1 - La licéité de la collecte

Ce principe, énoncé à l'article 4 de la loi « *Toute collecte de données ne peut être entreprise que d'une manière licite* », découle de la Convention du Conseil de l'Europe pour la protection des données.

Cette norme du comportement exprime le principe général de loyauté qui doit s'appliquer non seulement au droit de collecter les données, mais aussi au mode de collecte. Ce qui signifie qu'en dehors d'une norme de droit matériel prévoyant une collecte de données ou en dehors du consentement de la personne concernée, aucune collecte de données n'est valable. En outre, celle-ci ne peut être effectuée qu'avec des procédés loyaux.

2 - Bonne foi du traitement

Un tel principe, qui découle du premier, est énoncé textuellement à l'article 2 : « *Le traitement doit être effectué conformément au principe de la bonne foi* ».

Ce principe signifie ici que la collecte de données doit avoir lieu **au su** de la personne concernée ou, à tout le moins, auprès d'elle. Celui qui recueille des données en trompant intentionnellement, en donnant de fausses indications quant au but du traitement ou en se présentant sous une fausse identité transgresse le principe de la bonne foi. Une telle collecte peut constituer une infraction pénale en cas d'astuce (Art. 179*bis* CP).

Pour les organes fédéraux, une condition supplémentaire est requise (Art. 15 LPD) : la collecte de données doit être effectuée de manière reconnaissable pour les personnes concernées.

3 - La proportionnalité du traitement

Ce principe également appelé « **la théorie du sacrifice exigible** » s'applique à l'étendue et aux catégories des données personnelles utilisées, de même qu'au mode de traitement. Il

faut définir clairement les intérêts publics visés et observer si, dans chaque cas, les données sont nécessaires à l'accomplissement d'une tâche légale. Si l'administration peut exécuter son travail sans traiter de données personnelles, elle doit renoncer à une telle collecte et à un tel traitement, car le traitement de ces données personnelles n'est pas la règle mais **l'exception fondée.** Il est donc interdit à l'administration de collecter des données « en prévision de ».

4 - La finalité du traitement

« *Les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances* ».

Énoncé à l'art. 4 al. 3 LPD, ce principe comporte deux éléments :

- la détermination d'une finalité préalable au traitement ;
- la détermination de la compatibilité de toute modification avec le but initial du traitement.

Ce principe est un élément de la transparence puisque la finalité de tout traitement de données doit être énoncée dans la base légale la justifiant ou se déduire des tâches légales des organes publics traitant les données.

5 - L'exactitude des données

Énoncé à l'art. 5 al. 1 LPD : « *Quiconque traite des données personnelles doit s'assurer qu'elles sont correctes* », ce principe s'interprète à la fois selon l'exigence de proportionnalité et en fonction de la finalité du traitement. C'est dire que la notion d'exactitude varie à la fois selon la personne, publique ou privée, qui traite les données et selon le type de données. Elle ne peut s'appliquer qu'aux données objectives, puisque les appréciations et les jugements de valeur relevant de la subjectivité échappent à tout classement de juste ou d'inexact. Dans ce cas, la personne concernée est autorisée à agir en justice afin d'exiger que soit mentionné le caractère litigieux d'une information, dès lors que ni l'exactitude, ni l'inexactitude de celle-ci n'est démontrée et ne peut l'être.

6 - Les conditions de la communication à l'étranger

« *Aucune donnée personnelle ne peut être communiquée à l'étranger si la personnalité des personnes concernées devait se trouver gravement menacée, notamment du fait de l'absence d'une protection des données équivalente de celle qui est garantie en Suisse* » (Art. 6 al 1 LPD). Cette disposition pose le principe de l'équivalence. Il s'agit d'assurer que dans les autres pays une protection des données soit au moins égale à celle du droit suisse. La loi règle le transfert des fichiers à l'étranger. Dans le cas où cette transmission s'effectue à l'insu des personnes concernées, pour autant qu'une telle communication ne découle pas d'une obligation légale, **une déclaration au Préposé fédéral à la protection des données est nécessaire**.

7 - La sécurité des données

Le maître du fichier est tenu de prendre des mesures spécifiques permettant de protéger les informations contre leur perte, leur falsification ou l'utilisation illicite durant les phases du traitement. L'Ordonnance d'application de la loi (OLPD) donne les instructions nécessaires à cet égard.

LA TRANSPARENCE VOULUE GRÂCE À LA PUBLICITÉ DES FICHIERS ET AU DROIT D'ACCÈS

Pour que chacun puisse avoir connaissance de l'existence d'un traitement de données le concernant, la loi instaure un registre des fichiers tenu par le Préposé fédéral à la protection des données et « *toute personne peut demander au maître d'un fichier si des données la concernant sont traitées* » (Art. 8 LPD). Le droit d'accès de la personne physique ou le droit d'accès de la personne morale sur les informations détenues ou utilisées par des tiers sur son compte est considéré comme « *l'institution clé de la protection des données* ». C'est l'utilisation du droit d'accès, véritable contrôle personnel, qui met en œuvre, si nécessaire, une correction soit volontaire, soit comme résultat d'une action en justice, des données contenues dans un fichier.

L'exercice du droit d'accès

Les modalités pratiques du droit d'accès sont réglées par la loi. **Ce droit imprescriptible**, puisqu'il découle du droit de la personnalité, ne peut être exercé que par le titulaire lui-même. Il n'est pas transmissible. Les ayants droit ne peuvent exiger l'accès que s'ils font valoir un droit propre fondé sur la nécessité d'exercer une maîtrise sur les données personnelles du défunt sans qu'un intérêt prépondérant de proches ou de tiers ne s'y oppose.

La demande d'accès doit être présentée par écrit, puisque le titulaire doit être en mesure de s'identifier – condition particulièrement importante pour les informations définies spécifiquement comme *profil de personnalité* –. La soustraction de telles données personnelles sensibles constitue une infraction pénale nouvelle (Art. 179 novies CP) et le maître du fichier a toute la responsabilité de cette vérification.

L'accès doit être accordé non seulement sur les données *nominatives* mais sur toutes celles qui rendent cette personne *identifiable* par le maître du fichier. Si des informations figurent sous un numéro attribué à une personne, il s'agit de données personnelles, puisque la reconstitution est facile à opérer.

Les renseignements doivent être fournis par écrit, soit en règle générale sous forme de *photocopie* et *gratuitement* (sauf si l'exercice du droit remonte à moins d'un an : dans ce cas CHF 300).

Les restrictions au droit d'accès

Tout d'abord, l'accès peut être refusé lorsqu'une *loi* au sens formel le prévoit ou lorsque les intérêts prépondérants d'un tiers ou du maître du fichier l'exigent. Ces derniers doivent fournir la preuve des motifs par lesquels ils justifient leur refus d'accès et cette pesée des intérêts en présence se fera dans un sens favorable au requérant. A l'égard des organes fédéraux, c'est l'intérêt public prépondérant qui entre en considération : sûreté intérieure ou extérieure de la Confédération, bonnes relations avec l'étranger, secret de l'instruction pénale, par exemple.

Enfin, le droit d'accès est plus souple pour les médias : les exceptions précitées sont élargies puisqu'il est nécessaire de sauvegarder l'existence d'une presse libre et indépendante. La protection de la personnalité se heurte ici au droit à l'information que cette information soit diffusée par quelque média que ce soit : presse, radio, télévision, vidéotexte, télétexte ou banques de données librement accessibles. Aussi, lorsque des données personnelles fournissent des indications *sur les sources d'information*, lorsqu'un droit de regard sur des *projets de publications* en résulterait ou lorsque serait compromise la *libre formation de l'opinion publique*, le média peut refuser, restreindre ou différer l'octroi de renseignements. Encore faut-il que le fichier dudit média ne soit utilisé que pour la partie rédactionnelle de la publication. **Ce privilège ne s'étend donc pas aux données utilisées pour des fins commerciales**, soit publicitaires ou vente de données.

Application de ces règles

Ces règles s'appliquent à toutes les données faisant l'objet d'un traitement : cette notion est très large et les moyens de traitement importent peu. Les opérations couvertes vont de la collecte à l'archivage ou à la destruction de données, soit à l'indication de la nature des données détruites.

A la différence de certaines lois étrangères, le traitement n'est pas limité à un moyen électronique ou automatique, mais doit avoir lieu dans une **certaine durée**. Si le nom d'une personne n'apparaît qu'une fois dans un virement bancaire par exemple, sans être répertorié ou conservé, il ne peut s'agir d'une donnée personnelle au sens de la loi.

CONTRÔLE ET SURVEILLANCE

La tâche de veiller à la mise en œuvre de la législation sur la protection des données a été confiée à un *organe de surveillance indépendant,* ce qui est exceptionnel dans la tradition administrative helvétique. Cela résulte de la mise à profit de l'expérience américaine et de l'observation du faible impact des législations sur la protection des données en l'absence d'un contrôle spécifique. Respectant toutefois notre ordre institutionnel qui répugne à ne confier qu'à une seule personne l'ensemble du contrôle, une *double institution* existe : le **Préposé fédéral** à la protection des données et une **Commission fédérale** de la protection des données.

Le Préposé fédéral à la protection des données

Nommé par le Conseil fédéral, le préposé est indépendant de celui-ci : « *Il s'acquitte de ses tâches de manière autonome… il établit les faits d'office ou à la demande de tiers* » (Art. 26, 27, 29 LPD). Dans tous les cas, le Préposé demeure libre d'agir ou non.

Ses attributions : le Préposé agit comme conseiller. Il se tient à la disposition des services fédéraux et cantonaux de même que de « *toutes les autres autorités ou personnes privées soumises à la législation fédérale sur la protection des données* ». Le Préposé est également médiateur : son rôle est de désamorcer les conflits entre les parties en présence, contribuant ainsi à décharger les tribunaux civils ou administratifs.

Enfin, **le rôle essentiel du Préposé est la tenue du Registre des fichiers**. Il reçoit les déclarations des autorités et des particuliers au moment de l'enregistrement du fichier. Il entreprend un examen sommaire de la licéité du traitement. Il veille à la publication dans la Feuille Fédérale de la liste des fichiers enregistrés et, lors de la communication de fichiers à l'étranger, il doit recevoir les déclarations de transmission et apprécier si celles-ci ne risquent pas de porter gravement atteinte à la personnalité des personnes concernées. Le Préposé doit, en outre, tenir à jour un répertoire des législations en vigueur dans le monde sur la protection des données afin de pouvoir procéder à cette évaluation des risques. S'il constate un refus intentionnel de déclarer les fichiers, le Préposé peut, s'il s'agit de personnes privées, déposer plainte pénale - l'obligation de déclarer constituant une contravention punissable des arrêts ou de l'amende - ou, s'il s'agit de fonctionnaires, pratiquer une dénonciation de manière à provoquer des sanctions disciplinaires.

La Commission fédérale de la protection des données

Véritable commission d'arbitrage et de recours destinée à décharger le Tribunal Fédéral, la Commission est composée de sept juges nommés par le Conseil fédéral selon des critères liés à la représentation des milieux intéressés et à la représentation linguistique. Préposé et Commission siègent dans des lieux différents. La Commission doit avoir accès à la documentation scientifique du Préposé et, à l'inverse, le Préposé doit recevoir communication de toutes les décisions de la Commission quand bien même celles-ci sont publiées dans la Jurisprudence des autorités administratives de la Confédération (JACC).

La surveillance sur le secteur privé

Le Préposé n'exerce sur le secteur privé qu'une surveillance limitée car il n'agit en règle générale qu'en qualité

de conseiller. Toutefois, la loi prévoit trois cas dans lesquels l'ouverture d'une enquête est possible :

- lors de l'enregistrement de fichiers,
- lors de la déclaration de communications de données à l'étranger,
- lorsqu'il s'agit d'erreurs de systèmes A cet égard, le Préposé peut exiger la collaboration du maître du fichier et, si celui-ci refuse, il peut déposer plainte pénale.

La surveillance sur le secteur public

Elle s'exerce dans trois domaines :

❑ **sur les organes fédéraux** : afin d'exercer un contrôle efficace, le pouvoir d'enquête dévolu au préposé ressemble à celui d'un magistrat instructeur. Il peut se faire présenter les traitements afin de vérifier les accès autorisés, les interconnexions de fichiers et les mesures de sécurité ainsi que les mesures prises pour assurer la destruction des données périmées. Le Préposé doit également collaborer avec l'Office fédéral de l'informatique réglant la coordination au sein de l'Administration fédérale. Il se prononce sur chaque projet d'automatisation dès le stade de la conception. S'il constate un traitement litigieux ou illicite, le Préposé invite l'organe fédéral à le modifier ou à le faire cesser par une *recommandation*.

❑ **sur les organes cantonaux** : ce n'est pas le Préposé, mais un organe spécifique à chaque canton qui est chargé de cette mission. Un tel organe de contrôle devrait, bien entendu, être indépendant de l'administration cantonale. Néanmoins, toutes les décisions cantonales de dernière instance peuvent être portées devant la Commission fédérale de protection des données.

❑ **dans le domaine de la protection de l'Etat** : la protection de l'Etat contre le crime organisé ou le terrorisme justifie le *pouvoir d'investigation* très étendu conféré au Préposé sur les traitements de données effectués par la Police fédérale. Ce pouvoir n'est pratiquement pas limité par les textes réglementaires.

Une Recommandation du Préposé fédéral

A titre d'exemple de ce qui précède sur la protection des données en Suisse et sur le rôle du Préposé, il faut lire la **Recommandation** publiée en novembre 1994 dans la Feuille Fédérale (FF n° 47 p. 407) : la **formule d'inscription** remplie par le **candidat locataire** auprès d'un **propriétaire** ou d'une **gérance d'immeuble** entre dans le champ d'application légal. Il ne s'agit pas en effet d'un usage exclusivement personnel de ces formules comportant de nombreuses indications sur le mode de vie, la situation financière et sur la personne de celui qui la remplit :

« *La récolte par le bailleur de données concernant des personnes intéressées en vue de sélectionner le futur locataire d'un logement déterminé est donc en principe, sous certaines conditions,* ***justifié****. Il importe toutefois que soient respectés le principe de licéité de la collecte de données, le principe de la bonne foi et de la proportionnalité du traitement, le principe du traitement dans le seul but qui est indiqué lors de la collecte des données ou qui ressort des circonstances et le principe de la sécurité des données... Il y a aussi atteinte à la personnalité lorsque des données sont traitées contre la volonté expresse de la personne concernée et lorsque des données sensibles ou des profils de la personnalité sont communiqués à des tiers.* ***Une atteinte à la personnalité est illicite à moins d'être justifiée par le consentement de la victime, par un intérêt prépondérant privé ou public, ou par la loi****.* »

Avant de fixer sa Recommandation et de la notifier aux associations de bailleurs et de locataires, le Préposé a précisé les deux points suivants :

• « *Un intérêt* ***prépondérant*** *de la personne qui traite les données personnelles entre notamment en considération si le traitement est en relation directe avec la conclusion ou l'exécution d'un* ***contrat*** *et si les données traitées concernent le cocontractant.* ***La collecte se justifie*** *dans la mesure où elle sert à choisir le locataire adéquat.* »

• « *Pour les données récoltées en vertu* ***d'obligations légales*** *du bailleur - soit l'obligation de transmettre certains renseignements au contrôle de l'habitant ou à la police des étrangers - le bailleur est en principe autorisé à les requérir* ***uniquement du locataire finalement choisi****, puisque l'obligation légale d'annoncer ne concerne que le locataire et non pas les candidats intéressés.* »

• « *Le Préposé a accordé un délai de trente jours aux destinataires de cette Recommandation pour déclarer si elles rejettent cette dernière.* » *En cas de rejet ou de non respect de la Recommandation,* « *le Préposé pourra soumettre le cas pour décision à la Commission fédérale de la protection des données.* »

*
* *

Il convient maintenant de savoir si les devoirs spécifiques institués par cette loi et qui se rapportent à l'exactitude et à la sécurité des données dans le but de protéger la personnalité contient une norme protectrice en cas de dommage purement économique. Le lésé qui invoquera un dommage immatériel (selon l'Art. 49 CO) devra prouver que le préjudice subi est d'une intensité suffisante pour justifier une compensation en argent.

Seule une jurisprudence satisfaisante, que nous attendons, permettra à ce texte légal de jouer à plein son rôle préventif. ■